

# RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Emitido em: 07/05/2026 às 09:12:58

A seguir reproduzimos todas as informações pertinentes ao tema privacidade e proteção de dados de acordo com os inventários presentes no GPD Governace que deve refletir os aspectos atuais escopo da Lei Geral de Proteção de Dados.

## Identificação do controlador

**CNPJ:** 97.676.693/0001-79

**Razão Social:** OMNISBLUE COMPLIANCE SERVICOS E PARTICIPACOES LTDA

**Endereço:** Santos

**Website:** <https://www.omnisblue.com>

**Área de atuação:** Serviço

**Tipo de atuação:** Privada

**Tipo de DPO:** Interno

**DPO Responsável:** Adilson Taub Jr

**Contato do DPO:** [adilson.taub@omnisblue.com](mailto:adilson.taub@omnisblue.com)

## Situação de adequação LGPD

A adequação à LGPD é um processo geralmente longo e quem é melhor executado quando dividido em etapas que se completam e que, não necessariamente são executadas de forma totalmente sequencial.

Atualmente as datas de controle de cada uma dessas etapas de adequação são:

### Etapa de Diagnóstico:

**Início:** Não Informado      **Encerramento:** Não Informado      **Responsável:** Anderson Mattiuci

### Etapa de Adequação:

**Início:** Não Informado      **Encerramento:** Não Informado      **Responsável:** Diego Silva dos Santos

### Etapa de Operação:

**Início:** Não Informado      **Encerramento:** Não Informado      **Responsável:** Adilson Taub Jr

## Parâmetros selecionados para geração deste DPIA

<b>Diretoria:</b> Não informado	<b>Área:</b> Não informado	<b>Departamento:</b> Não informado
<b>Hipótese:</b> Não informado	<b>Papel:</b> Não informado	<b>Operador:</b> Não informado
<b>Ativo:</b> Não informado	<b>Finalidade:</b> Não informado	<b>Somente Finalidades com alto impacto?:</b> Não

## Tratamento de dados pessoais

A seguir são listados todos os tratamentos de dados pessoais atualmente em execução pelo controlador suas hipóteses de tratamento previstas na LGPD, seus fundamentos legais em quais ativos de informação esses tratamentos são realizados:

### Finalidade: Coletar fotos de candidatos

<b>Hipótese de tratamento (LGPD):</b> Art. 7º, I - Consentimento do Titular	<b>Papel da entidade:</b> Controlador
<b>Trata dados sensíveis?</b> Não	<b>Trata dados de crianças/adolescentes?:</b> Não
<b>Origem da Informação:</b> Candidato	<b>Destino da Informação:</b> RH
<b>Frequência:</b> Média (semanalmente)	<b>Volumetria:</b> Médio (500 - 999)
<b>Finalidade de alto impacto ?:</b> Não	

## Salvaguardas

**Ativo:** Dynamics 365

**Medida técnica:** Pseudonimização e anonimização

Descrição da Medida Técnica: Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

**Ativo:** Dynamics 365

**Medida técnica:** Controle de acesso

Descrição da Medida Técnica: Restrição do acesso aos dados pessoais apenas aos colaboradores autorizados e com necessidade de conhecer as informações. Implementação de mecanismos de autenticação e autorização robustos.

**Ativo:** Dynamics 365

**Medida técnica:** Backup

Descrição da Medida Técnica: Completo: Cria uma cópia completa de todos os dados em um determinado momento. Incremental: Cria cópias apenas dos dados que foram alterados desde o último backup completo. Diferencial: Cria cópias de todos os dados que foram alterados desde o último backup incremental. Mirror: Cria uma cópia exata dos dados em tempo real, como um espelho.

**Ativo:** Dynamics 365

**Medida técnica:** Firewalls

Descrição da Medida Técnica: Primeira linha de defesa: Filtra o tráfego de rede, permitindo apenas o acesso autorizado. Tipos: Firewalls de rede, de aplicativos e de próxima geração. Funcionalidades: Bloqueio de portas, inspeção de pacotes, prevenção de intrusão.

**Ativo:** Dynamics 365

**Medida técnica:** Autenticação Multifator

Descrição da Medida Técnica: Segurança adicional: Requer mais de uma forma de verificação de identidade, como senha, token e biometria. Tipos: Autenticação baseada em conhecimento, posse e características inerentes.

**Ativo:** Dynamics 365

**Medida técnica:** Security Robot 2.0

Descrição da Medida Técnica: Security Robot 2.0

**Ativo:** Dynamics 365

**Medida técnica:** Criptografia

Descrição da Medida Técnica: Proteção dos dados em trânsito e em repouso através da transformação em códigos indecifráveis sem a chave correta.

**Ativo:** Dynamics 365

**Medida técnica:** Balanceamento de Carga

Descrição da Medida Técnica: Distribuir o tráfego de rede entre vários servidores para evitar sobrecarga em um único servidor e garantir a disponibilidade e o desempenho dos serviços.

## Riscos

**Título do Risco:** Período de Retenção Excessivo dos Dados dos Candidatos Não Contratados

Descrição do Risco: risco: Reter currículos e dados de candidatos não selecionados por um período indefinido ou excessivamente longo, sem uma justificativa clara (ex: banco de talentos para futuras vagas com consentimento explícito e prazo definido).

**Status:** Encontrado

**Criticidade:** Moderada

## Fundamentos Legais

Dados não cadastrado

## Sobre os dados em tratamento

**Artefatos:** Certidão de Nascimento

**Lista de dados pessoais tratados na finalidade:**

- Data | de nascimento | Cadastral | Imprescindível para o tratamento? Sim
- Nome | da mãe | Cadastral | Imprescindível para o tratamento? Sim
- Nome | do pai | Cadastral | Imprescindível para o tratamento? Sim
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Sim

**Artefatos:** CPF

**Lista de dados pessoais tratados na finalidade:**

- Data | de emissão | Cadastral | Imprescindível para o tratamento? Sim
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Sim
- Número | do CPF | Cadastral | Imprescindível para o tratamento? Sim

## Sobre o processo de consentimento

**O tratamento depende de consentimento:** Sim

**Processo de obtenção de consentimento:** Coletar consentimentos para cadastro de dependentes

## Sobre operadores associados

**Utiliza Operador?** Sim

**Operadores:** Não Informado

Dados não cadastrado

### Sobre o compartilhamento de informações

Os dados são compartilhados? Não

Como os dados são compartilhados: Não Informado

Com quem os dados são compartilhados

Dados não cadastrados

Realiza transferências internacionais ? Não

### Sobre o fim do tratamento dos dados

Os dados são descartados? Não

Prazo de armazenamento: Não Informado

Processo de descarte:

Processo de descarte de dados para finalidades com consentimento

### Sobre os ativos de informação utilizados

Esse tratamento de dados é executado nos seguintes ativos de informação:

Ativos de informação associados ao tratamento de dados

Título do ativo: Dynamics 365

Tipo: Eletrônico

### Sobre os riscos associados

Esse tratamento de dados está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados à finalidade de tratamento de dados:

Título do risco: Período de Retenção Excessivo dos Dados dos Candidatos Não Contratados

**Finalidade:** Coletar dados dos filhos dos dependentes

**Hipótese de tratamento (LGPD):** Art. 7º, II - Obrigação Legal ou Regulatória

**Papel da entidade:** Controlador

**Trata dados sensíveis?** Não

**Trata dados de crianças/adolescentes?:** Não

**Origem da Informação:** Não Informado

**Destino da Informação:** Não Informado

**Frequência:** Não Informado

**Volumetria:** Não Informado

**Finalidade de alto impacto ?:** Não

### Salvaguardas

**Ativo:** OMIE - ERP Financeiro

**Medida técnica:** Pseudonimização e anonimização

Descrição da Medida Técnica: Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

**Ativo:** OMIE - ERP Financeiro

**Medida técnica:** Controle de acesso

Descrição da Medida Técnica: Restrição do acesso aos dados pessoais apenas aos colaboradores autorizados e com necessidade de conhecer as informações. Implementação de mecanismos de autenticação e autorização robustos.

**Ativo:** OMIE - ERP Financeiro

**Medida técnica:** Backup

Descrição da Medida Técnica: Completo: Cria uma cópia completa de todos os dados em um determinado momento. Incremental: Cria cópias apenas dos dados que foram alterados desde o último backup completo. Diferencial: Cria cópias de todos os dados que foram alterados desde o último backup incremental. Espelho: Cria uma cópia exata dos dados em tempo real, como um espelho.

**Ativo:** OMIE - ERP Financeiro

**Medida técnica:** Firewalls

Descrição da Medida Técnica: Primeira linha de defesa: Filtra o tráfego de rede, permitindo apenas o acesso autorizado.  
Tipos: Firewalls de rede, de aplicativos e de próxima geração. Funcionalidades: Bloqueio de portas, inspeção de pacotes, prevenção de intrusão.

**Ativo:** OMIE - ERP Financeiro

**Medida técnica:** Autenticação Multifator

Descrição da Medida Técnica: Segurança adicional: Requer mais de uma forma de verificação de identidade, como senha, token e biometria. Tipos: Autenticação baseada em conhecimento, posse e características inerentes.

**Ativo:** OMIE - ERP Financeiro

**Medida técnica:** Security Robot 2.0

Descrição da Medida Técnica: Security Robot 2.0

**Ativo:** Privacy Portal

**Medida técnica:** Security Robot 2.0

Descrição da Medida Técnica: Security Robot 2.0

**Ativo:** Privacy Portal

**Medida técnica:** Gerenciamento de Incidentes e ameaças

Descrição da Medida Técnica: Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

## Riscos

Dados não cadastrado

## Fundamentos Legais

Dados não cadastrado

## Sobre os dados em tratamento

Dados não cadastrado

## Sobre o processo de consentimento

O tratamento depende de consentimento: Não

## Sobre operadores associados

Utiliza Operador? Não

Operadores: Não Informado

Dados não cadastrado

## Sobre o compartilhamento de informações

Os dados são compartilhados? Não

Como os dados são compartilhados: Não Informado

Com quem os dados são compartilhados

Dados não cadastrados

Realiza transferências internacionais ? Não

## Sobre o fim do tratamento dos dados

**Os dados são descartados?** Não

**Prazo de armazenamento:** Não Informado

**Processo de descarte:**

**Dados não cadastrado**

#### **Sobre os ativos de informação utilizados**

Esse tratamento de dados é executado nos seguintes ativos de informação:

Ativos de informação associados ao tratamento de dados

**Título do ativo:** OMIE - ERP Financeiro

**Tipo:** Eletrônico

**Título do ativo:** Privacy Portal

**Tipo:** Eletrônico

#### **Sobre os riscos associados**

Esse tratamento de dados está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados à finalidade de tratamento de dados:

**Dados não cadastrado**

## Medidas administrativas de segurança

A seguir são listadas todas as medidas administrativas (políticas) atualmente em vigor na empresa, onde são documentados os compromissos do controlador com a privacidade dos Titulares de Dados Pessoais:

### Política: Manual de Segurança da Informação

Tipo da política: Interna

Início de vigência: 04/05/2026

Fim da vigência: 31/05/2028

Responsável atual pela política: Adilson Taub Jr

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

### Política: 02 - Guia de Medidas Técnicas de Segurança (V1.2)

Tipo da política: Interna

Início de vigência: 06/05/2026

Fim da vigência: 30/05/2030

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

### Política: 03 - Guia de Gerenciamento das Políticas de Segurança da Informação (V1.1)

Tipo da política: Interna

Início de vigência: 05/05/2026

Fim da vigência: 30/05/2029

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

### Política: 04 - Política de Segurança em Estações de Trabalho e Recursos de Computação Móvel (V1.0)

Tipo da política: Interna

Início de vigência: 06/05/2026

Fim da vigência: 22/05/2030

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

#### Política: 05 - Política de Segurança Aplicada às Pessoas (V1.0)

Tipo da política: Interna

Início de vigência: 04/05/2026

Fim da vigência: 22/05/2030

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

#### Política: 06 - Política de Classificação da Informação (V1.0)

Tipo da política: Interna

Início de vigência: 04/05/2026

Fim da vigência: 29/05/2030

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

#### Política: 07 - Política de Descarte de Dados (V1.0)

Tipo da política: Interna

Início de vigência: 06/05/2026

Fim da vigência: 30/05/2029

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não  
Abrange compartilhamento de dados pessoais? Não

#### Política: 08 - Guia de Premissas e Padrões de Desenvolvimento de Software (V1.2)

Tipo da política: Interna

Início de vigência: 04/05/2026

Fim da vigência: 23/05/2029

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

#### Política: 09 - Política de privacidade (V1.3)

Tipo da política: Interna

Início de vigência: 04/05/2026

Fim da vigência: 29/05/2030

Responsável atual pela política: Anderson Mattiuci

Tem processo de manutenção? Não

Título do processo de manutenção: Não Informado

#### Análise dos parâmetros da política

Integra Governança? Não

Está completa? Não

É exequível? Não

Trata o papel do Titular? Não

Trata o papel do DPO? Não

Trata Operadores? Não

Abrange o processo de gestão de riscos? Não

Abrange o processo de gestão de incidentes? Não

Abrange compartilhamento de dados pessoais? Não

## Medidas técnicas de segurança

A seguir são listadas todas as medidas técnicas atualmente implementadas em cada ativo da informação utilizado para a realização de rotinas de tratamento de dados pessoais e o nível de Confiabilidade desses ativos e acordo com as atuais medidas técnicas em vigor:

#### Ativo da informação: OMIE - ERP Financeiro

Tipo do ativo: Eletrônico

Subtipo: BPMS/Workflow

Tecnologia envolvida: Java, Oracle

Fornecedor atual: Não Informado

Responsável atual pela gestão do ativo: Sérgio Angrisano

#### Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias)

Nível de Integridade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias) Backups Regulares e Recuperação dos Backups, Testes regulares de recuperação

dos backups

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias) Testes regulares de recuperação dos backups

#### Sobre as medidas técnicas de segurança implementadas no ativo

**Medida técnica:** Pseudonimização e anonimização

Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

**Medida técnica:** Controle de acesso

Restrição do acesso aos dados pessoais apenas aos colaboradores autorizados e com necessidade de conhecer as informações. Implementação de mecanismos de autenticação e autorização robustos.

**Medida técnica:** Backup

Completo: Cria uma cópia completa de todos os dados em um determinado momento. Incremental: Cria cópias apenas dos dados que foram alterados desde o último backup completo. Diferencial: Cria cópias de todos os dados que foram alterados desde o último backup incremental. Espelho: Cria uma cópia exata dos dados em tempo real, como um espelho.

**Medida técnica:** Firewalls

Primeira linha de defesa: Filtra o tráfego de rede, permitindo apenas o acesso autorizado. Tipos: Firewalls de rede, de aplicativos e de próxima geração. Funcionalidades: Bloqueio de portas, inspeção de pacotes, prevenção de intrusão.

**Medida técnica:** Autenticação Multifator

Segurança adicional: Requer mais de uma forma de verificação de identidade, como senha, token e biometria. Tipos: Autenticação baseada em conhecimento, posse e características inerentes.

**Medida técnica:** Security Robot 2.0

Security Robot 2.0

#### Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

- Senhas fracas
- Acesso indevido ao sistema OMIE
- Risco de Due Diligence referente ao fornecedor: Lotorian Tecnologia LTDA - CNPJ: 840.332.800-00124
- Risco de Due Diligence referente ao fornecedor: Omnisblue - CNPJ: 290.045.720-00120

**Ativo da informação:** Netsac - CRM

**Tipo do ativo:** Eletrônico

**Subtipo:** BPMS/Workflow

**Tecnologia envolvida:** C#, JavaScript

**Fornecedor atual:** Não Informado

**Responsável atual pela gestão do ativo:** Anderson Mattiuci

#### Sobre o nível de confiabilidade do ativo

**Nível geral de Confiabilidade do Ativo:** Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias)

Nível de Integridade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias) Criptografia dos Backups

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias) Backups Regulares e Recuperação dos Backups, Testes regulares de recuperação dos backups, Criptografia dos Backups, Redundância dos Backups, Listas de controle de acesso (ACLs)

#### Sobre as medidas técnicas de segurança implementadas no ativo

**Medida técnica:** Pseudonimização e anonimização

Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

**Medida técnica:** Controle de acesso

Restrição do acesso aos dados pessoais apenas aos colaboradores autorizados e com necessidade de conhecer as informações. Implementação de mecanismos de autenticação e autorização robustos.

**Medida técnica:** Backup

Completo: Cria uma cópia completa de todos os dados em um determinado momento. Incremental: Cria cópias apenas dos dados que foram alterados desde o último backup completo. Diferencial: Cria cópias de todos os dados que foram alterados desde o último backup incremental. Espelho: Cria uma cópia exata dos dados em tempo real, como um espelho.

**Medida técnica:** Firewalls

Primeira linha de defesa: Filtra o tráfego de rede, permitindo apenas o acesso autorizado. Tipos: Firewalls de rede, de aplicativos e de próxima geração. Funcionalidades: Bloqueio de portas, inspeção de pacotes, prevenção de intrusão.

**Medida técnica:** Autenticação Multifator

Segurança adicional: Requer mais de uma forma de verificação de identidade, como senha, token e biometria. Tipos: Autenticação baseada em conhecimento, posse e características inerentes.

**Medida técnica:** Security Robot 2.0

Security Robot 2.0

**Medida técnica:** Balanceamento de Carga

Distribuir o tráfego de rede entre vários servidores para evitar sobrecarga em um único servidor e garantir a disponibilidade e o desempenho dos serviços.

**Medida técnica:** Gerenciamento de Incidentes e ameaças

Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

#### Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

- Senhas fracas
- Falta de backup automático

**Ativo da informação:** Dynamics 365

**Tipo do ativo:** Eletrônico

**Subtipo:** BPMS/Workflow

**Tecnologia envolvida:** Não Informado

**Fornecedor atual:** Não Informado

**Responsável atual pela gestão do ativo:** Anderson Mattiuci

#### Sobre o nível de confiabilidade do ativo

**Nível geral de Confiabilidade do Ativo:** Baixo

Nível de Confidencialidade das informações tratadas pelo ativo: Baixo

- Não Informado

Nível de Integridade das informações tratadas pelo ativo: Baixo

- Não Informado

Nível de Disponibilidade das informações tratadas pelo ativo: Baixo

- Não Informado

### Sobre as medidas técnicas de segurança implementadas no ativo

**Medida técnica:** Pseudonimização e anonimização

Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

**Medida técnica:** Controle de acesso

Restrição do acesso aos dados pessoais apenas aos colaboradores autorizados e com necessidade de conhecer as informações. Implementação de mecanismos de autenticação e autorização robustos.

**Medida técnica:** Backup

Completo: Cria uma cópia completa de todos os dados em um determinado momento. Incremental: Cria cópias apenas dos dados que foram alterados desde o último backup completo. Diferencial: Cria cópias de todos os dados que foram alterados desde o último backup incremental. Espelho: Cria uma cópia exata dos dados em tempo real, como um espelho.

**Medida técnica:** Firewalls

Primeira linha de defesa: Filtra o tráfego de rede, permitindo apenas o acesso autorizado. Tipos: Firewalls de rede, de aplicativos e de próxima geração. Funcionalidades: Bloqueio de portas, inspeção de pacotes, prevenção de intrusão.

**Medida técnica:** Autenticação Multifator

Segurança adicional: Requer mais de uma forma de verificação de identidade, como senha, token e biometria. Tipos: Autenticação baseada em conhecimento, posse e características inerentes.

**Medida técnica:** Security Robot 2.0

Security Robot 2.0

**Medida técnica:** Criptografia

Proteção dos dados em trânsito e em repouso através da transformação em códigos indecifráveis sem a chave correta.

**Medida técnica:** Balanceamento de Carga

Distribuir o tráfego de rede entre vários servidores para evitar sobrecarga em um único servidor e garantir a disponibilidade e o desempenho dos serviços.

### Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

- Senhas fracas
- Acesso indevido ao sistema OMIE

**Ativo da informação:** Privacy Portal

**Tipo do ativo:** Eletrônico

**Subtipo:** Plataforma de controle de acesso

**Tecnologia envolvida:** Script Case , HTML, AJAX, CSS

**Fornecedor atual:** Não Informado

**Responsável atual pela gestão do ativo:** Anderson Mattiuci

#### Sobre o nível de confiabilidade do ativo

**Nível geral de Confiabilidade do Ativo:** Alto

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias)

Nível de Integridade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias) Criptografia dos Backups, Redundância dos Backups

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- (O Ativo não possui medidas obrigatórias) Backups Regulares e Recuperação dos Backups, Testes regulares de recuperação dos backups, Criptografia dos Backups, Redundância dos Backups

#### Sobre as medidas técnicas de segurança implementadas no ativo

**Medida técnica:** Security Robot 2.0

Security Robot 2.0

**Medida técnica:** Gerenciamento de Incidentes e ameaças

Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

#### Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

**Dados não cadastrado**

**Ativo da informação:** System Saúde

**Tipo do ativo:** Eletrônico

**Subtipo:** BPMS/Workflow

**Tecnologia envolvida:** Não Informado

**Fornecedor atual:** Não Informado

**Responsável atual pela gestão do ativo:** Anderson Mattiuci

#### Sobre o nível de confiabilidade do ativo

**Nível geral de Confiabilidade do Ativo:** Não Informado

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de confidencialidade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

Nível de Integridade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de integridade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- O ativo é um SAAS e toda a parte de disponibilidade do serviço é gerenciada pela fornecedora que possui suas próprias regras com relação a este serviço.

#### Sobre as medidas técnicas de segurança implementadas no ativo

**Medida técnica:** Security Robot 2.0

Security Robot 2.0

## Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

- Falta de política de privacidade

## Ativo da informação: Dynamics Sales

**Tipo do ativo:** Eletrônico

**Subtipo:** ERP

**Tecnologia envolvida:** MS Dynamics 365

**Fornecedor atual:** People Search Ltda

**Responsável atual pela gestão do ativo:** Sérgio Angrisano

## Sobre o nível de confiabilidade do ativo

**Nível geral de Confiabilidade do Ativo:** Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- Nível de confidencialidade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

Nível de Integridade das informações tratadas pelo ativo: Médio

- Nível de integridade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- Nível de disponibilidade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

## Sobre as medidas técnicas de segurança implementadas no ativo

**Medida técnica:** Medida técnica da Excelsior

**Medida técnica:** Security Robot 2.0

Security Robot 2.0

**Medida técnica:** Backups Regulares e Recuperação dos Backups

Consiste em copiar os dados importantes para um local seguro (físico ou na nuvem) em intervalos regulares. A recuperação de backups permite restaurar os dados em caso de perda, corrupção ou desastres.

**Medida técnica:** Testes regulares de recuperação dos backups

Além de fazer backups, é crucial testar periodicamente a restauração desses backups para garantir que eles estejam funcionando corretamente e que os dados possam ser recuperados em caso de necessidade.

**Medida técnica:** Criptografia dos Backups

Criptografar os backups adiciona uma camada extra de segurança, protegendo os dados mesmo se o local de armazenamento for comprometido.

**Medida técnica:** Recaptha

Um sistema de verificação para distinguir entre humanos e robôs, utilizado para prevenir ataques automatizados, como bots de spam ou brute-force.

**Medida técnica:** Logs de auditoria detalhados

Registram as atividades realizadas nos sistemas, como logins, alterações em dados, acessos a recursos, etc. Esses logs são essenciais para investigar incidentes de segurança e identificar possíveis violações.

**Medida técnica:** Monitoramento contínuo e alertas em tempo real

Monitora constantemente os sistemas em busca de atividades suspeitas ou anomalias e gera alertas em tempo real para que as equipes de segurança possam agir rapidamente.

**Medida técnica:** Criptografia de Dados em Trânsito

Criptografa os dados que estão sendo transmitidos entre sistemas ou dispositivos, protegendo-os contra interceptação durante a transmissão. Exemplos: HTTPS, VPN.

**Medida técnica:** Gerenciamento de Chaves criptográficas

Define políticas e procedimentos para a geração, armazenamento, distribuição e revogação de chaves criptográficas, garantindo a segurança dos dados criptografados.

**Medida técnica:** DLP (Data Loss Prevention)

Conjunto de técnicas e ferramentas para prevenir a perda ou o vazamento de dados sensíveis, monitorando o tráfego de dados e bloqueando transferências não autorizadas.

**Medida técnica:** Redundância dos Backups

Manter cópias dos backups em locais diferentes (redundância geográfica) aumenta a resiliência contra desastres naturais ou falhas em um único local.

**Medida técnica:** Listas de controle de acesso (ACLs)

ACLs definem permissões de acesso a recursos específicos (arquivos, diretórios, etc.), controlando quem pode ler, escrever ou executar cada recurso.

**Medida técnica:** Controle de Acesso Baseado em Funções (RBAC)

Define permissões de acesso com base nos papéis ou funções dos usuários na organização, simplificando o gerenciamento de permissões e garantindo que cada usuário tenha apenas o acesso necessário para realizar suas tarefas.

**Medida técnica:** Gestão e controle de versões

Manter um histórico das diferentes versões de software e aplicações, permitindo reverter para versões anteriores em caso de problemas ou vulnerabilidades.

**Medida técnica:** Treinamento de Segurança para Funcionários

Educar os funcionários sobre as melhores práticas de segurança da informação, como senhas fortes, phishing, engenharia social, etc.

**Medida técnica:** Plano de Recuperação de Desastres

Documentar procedimentos para restaurar os sistemas e dados em caso de um desastre (incêndio, inundação, etc.), minimizando o tempo de inatividade e a perda de dados.

**Medida técnica:** Contratos de Nível de Serviço (SLAs)

Acordos entre o provedor de serviços e o cliente que definem os níveis de serviço esperados, incluindo tempo de resposta a incidentes de segurança, tempo de inatividade permitido, etc.

**Medida técnica:** Pseudonimização e anonimização

Pseudonimização: Substituição de identificadores diretos por identificadores únicos, dificultando a associação dos dados a um indivíduo específico. Anonimização: Remoção de informações que permitam a identificação direta ou indireta do indivíduo, tornando os dados irreversíveis.

**Medida técnica:** Gerenciamento de Incidentes e ameaças

Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

### Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

**Dados não cadastrado**

**Ativo da informação: Servidor Local****Tipo do ativo:** Eletrônico**Subtipo:** Servidor de arquivo**Tecnologia envolvida:** Não Informado**Fornecedor atual:** TECH Talent informatica Ltda**Responsável atual pela gestão do ativo:** Jonas Evangelista da Silva**Sobre o nível de confiabilidade do ativo****Nível geral de Confiabilidade do Ativo:** Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- Nível de confidencialidade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

Nível de Integridade das informações tratadas pelo ativo: Alto

- Nível de integridade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- Nível de disponibilidade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

**Sobre as medidas técnicas de segurança implementadas no ativo****Medida técnica:** Backups Regulares e Recuperação dos Backups

Consiste em copiar os dados importantes para um local seguro (físico ou na nuvem) em intervalos regulares. A recuperação de backups permite restaurar os dados em caso de perda, corrupção ou desastres.

**Medida técnica:** Testes regulares de recuperação dos backups

Além de fazer backups, é crucial testar periodicamente a restauração desses backups para garantir que eles estejam funcionando corretamente e que os dados possam ser recuperados em caso de necessidade.

**Medida técnica:** Criptografia dos Backups

Criptografar os backups adiciona uma camada extra de segurança, protegendo os dados mesmo se o local de armazenamento for comprometido.

**Medida técnica:** Listas de controle de acesso (ACLs)

ACLs definem permissões de acesso a recursos específicos (arquivos, diretórios, etc.), controlando quem pode ler, escrever ou executar cada recurso.

**Medida técnica:** Recaptha

Um sistema de verificação para distinguir entre humanos e robôs, utilizado para prevenir ataques automatizados, como bots de spam ou brute-force.

**Medida técnica:** Logs de acesso

Registram as tentativas de acesso aos sistemas, incluindo logins bem-sucedidos e falhos. São úteis para monitorar atividades suspeitas e identificar tentativas de acesso não autorizado.

**Medida técnica:** Monitoramento contínuo e alertas em tempo real

Monitora constantemente os sistemas em busca de atividades suspeitas ou anomalias e gera alertas em tempo real para que as equipes de segurança possam agir rapidamente.

**Medida técnica:** Criptografia de Dados em Repouso

Criptografa os dados armazenados em dispositivos de armazenamento (HDs, SSDs, etc.), protegendo-os contra acessos não autorizados em caso de roubo ou perda dos dispositivos.

**Medida técnica:** Gerenciamento de Chaves criptográficas

Define políticas e procedimentos para a geração, armazenamento, distribuição e revogação de chaves criptográficas, garantindo a segurança dos dados criptografados.

**Medida técnica:** Implementação de soluções de redundância para componentes críticos (servidores, redes, armazenamento).

Duplicar componentes críticos da infraestrutura para garantir a disponibilidade dos serviços em caso de falha de um dos

componentes (servidores, redes, armazenamento).

**Medida técnica:** Atualizações e Patches

Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas operacionais.

**Medida técnica:** Treinamento de Segurança para Funcionários

Educar os funcionários sobre as melhores práticas de segurança da informação, como senhas fortes, phishing, engenharia social, etc.

**Medida técnica:** Plano de Recuperação de Desastres

Documentar procedimentos para restaurar os sistemas e dados em caso de um desastre (incêndio, inundação, etc.), minimizando o tempo de inatividade e a perda de dados.

**Medida técnica:** Contratos de Nível de Serviço (SLAs)

Acordos entre o provedor de serviços e o cliente que definem os níveis de serviço esperados, incluindo tempo de resposta a incidentes de segurança, tempo de inatividade permitido, etc.

**Medida técnica:** Análise de Vulnerabilidades

Realizar testes e varreduras para identificar vulnerabilidades de segurança nos sistemas e aplicações, permitindo corrigi-las antes que sejam exploradas por invasores.

**Medida técnica:** Gerenciamento de Incidentes e ameaças

Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

### Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

- Notificação na empresa sobre vazamento de dados
- Risco de Due Diligence referente ao fornecedor: People Search Ltda - CNPJ: 263.655.080-00187
- (Assistant) - Contrato com vigência expirada: Certificado Iso
- Expiração de senha superior a 90 dias
- Ativo sem medidas técnicas atreladas

### Ativo da informação: Sistema Legado de Folha de Pagamento

**Tipo do ativo:** Eletrônico

**Subtipo:** ERP

**Tecnologia envolvida:** Não Informado

**Fornecedor atual:** Não Informado

**Responsável atual pela gestão do ativo:** Anderson Mattiuci

### Sobre o nível de confiabilidade do ativo

**Nível geral de Confiabilidade do Ativo:** Alto

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- Nível de confidencialidade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

Nível de Integridade das informações tratadas pelo ativo: Alto

- Nível de integridade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

Nível de Disponibilidade das informações tratadas pelo ativo: Alto

- Nível de disponibilidade gerado através do cálculo da CID, com base nas medidas padrões selecionadas.

## Sobre as medidas técnicas de segurança implementadas no ativo

### **Medida técnica:** Backups Regulares e Recuperação dos Backups

Consiste em copiar os dados importantes para um local seguro (físico ou na nuvem) em intervalos regulares. A recuperação de backups permite restaurar os dados em caso de perda, corrupção ou desastres.

### **Medida técnica:** Testes regulares de recuperação dos backups

Além de fazer backups, é crucial testar periodicamente a restauração desses backups para garantir que eles estejam funcionando corretamente e que os dados possam ser recuperados em caso de necessidade.

### **Medida técnica:** Redundância dos Backups

Manter cópias dos backups em locais diferentes (redundância geográfica) aumenta a resiliência contra desastres naturais ou falhas em um único local.

### **Medida técnica:** Autenticação multifator (MFA)

Exige mais de uma forma de autenticação para acessar um sistema ou recurso, como senha e código enviado por SMS ou aplicativo autenticador, aumentando a segurança contra acessos não autorizados.

### **Medida técnica:** Recaptha

Um sistema de verificação para distinguir entre humanos e robôs, utilizado para prevenir ataques automatizados, como bots de spam ou brute-force.

### **Medida técnica:** Logs de auditoria detalhados

Registram as atividades realizadas nos sistemas, como logins, alterações em dados, acessos a recursos, etc. Esses logs são essenciais para investigar incidentes de segurança e identificar possíveis violações.

### **Medida técnica:** Criptografia de Dados em Trânsito

Criptografa os dados que estão sendo transmitidos entre sistemas ou dispositivos, protegendo-os contra interceptação durante a transmissão. Exemplos: HTTPS, VPN.

### **Medida técnica:** DLP (Data Loss Prevention)

Conjunto de técnicas e ferramentas para prevenir a perda ou o vazamento de dados sensíveis, monitorando o tráfego de dados e bloqueando transferências não autorizadas.

### **Medida técnica:** Balanceamento de Carga

Distribuir o tráfego de rede entre vários servidores para evitar sobrecarga em um único servidor e garantir a disponibilidade e o desempenho dos serviços.

### **Medida técnica:** Atualizações e Patches

Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas operacionais.

### **Medida técnica:** Contratos de Nível de Serviço (SLAs)

Acordos entre o provedor de serviços e o cliente que definem os níveis de serviço esperados, incluindo tempo de resposta a incidentes de segurança, tempo de inatividade permitido, etc.

### **Medida técnica:** Análise de Vulnerabilidades

Realizar testes e varreduras para identificar vulnerabilidades de segurança nos sistemas e aplicações, permitindo corrigi-las antes que sejam exploradas por invasores.

### **Medida técnica:** Gerenciamento de Incidentes e ameaças

Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

### **Medida técnica:** Criptografia dos Backups

Criptografar os backups adiciona uma camada extra de segurança, protegendo os dados mesmo se o local de armazenamento for comprometido.

**Medida técnica:** Logs de acesso

Registram as tentativas de acesso aos sistemas, incluindo logins bem-sucedidos e falhos. São úteis para monitorar atividades suspeitas e identificar tentativas de acesso não autorizado.

**Medida técnica:** Monitoramento contínuo e alertas em tempo real

Monitora constantemente os sistemas em busca de atividades suspeitas ou anomalias e gera alertas em tempo real para que as equipes de segurança possam agir rapidamente.

**Medida técnica:** Ferramentas de detecção de falhas

Utilizam técnicas e algoritmos para identificar possíveis falhas de segurança nos sistemas, como vulnerabilidades em softwares ou configurações incorretas.

**Medida técnica:** Criptografia de Dados em Repouso

Criptografa os dados armazenados em dispositivos de armazenamento (HDs, SSDs, etc.), protegendo-os contra acessos não autorizados em caso de roubo ou perda dos dispositivos.

**Medida técnica:** Configuração de mecanismos de failover automatizado para garantir a continuidade do serviço em caso de falhas.

Implementar sistemas que automaticamente direcionam o tráfego para um sistema redundante em caso de falha do sistema principal, minimizando o tempo de inatividade.

**Medida técnica:** Gestão e controle de versões

Manter um histórico das diferentes versões de software e aplicações, permitindo reverter para versões anteriores em caso de problemas ou vulnerabilidades.

### Sobre os riscos associados

Esse ativo da informação está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados ao ativo da informação:

**Dados não cadastrado**

## Gestão de riscos de privacidade e segurança da informação

Para a gestão de riscos de privacidade e segurança da informação, utilizamos a seguinte matriz estruturada para classificação da criticidade de cada risco, que é composta de acordo com a classificação de impacto do risco e sua probabilidade percentual em ocorrer:

		Impacto		
		Baixo	Média	Alto
Probabilidade	100%	Alta	Urgente	Urgente
	90%	Moderada	Urgente	Urgente
	80%	Moderada	Alta	Urgente
	70%	Moderada	Alta	Urgente
	60%	Moderada	Alta	Alta
	50%	Baixa	Alta	Alta
	40%	Baixa	Moderada	Alta
	30%	Baixa	Moderada	Moderada
	20%	Baixa	Baixa	Moderada
	10%	Baixa	Baixa	Moderada

A seguir são listados todos os atuais riscos de privacidade e proteção de dados identificados e que estão sendo gerenciados pelo controlador, ordenados de acordo com sua criticidade:

### Risco: Acesso indevido ao sistema OMIE

**Criticidade:** Alta

**Classificação de impacto:** Médio

**% de probabilidade de ocorrência:** 80%

**Personas afetadas pelo risco:** Titulares

**Status atual:** Encontrado

**Data de registro:** 04/08/2024

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Anderson Mattiuci

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Cadastrar dependentes
- Fechamento de folha para terceiros
- Recrutamento e Seleção

**Tratamento de dados pessoais associados ao risco:**

- Cadastrar dependentes
- Realizar Recrutamento de seleção

**Ativos da informação associados ao risco:**

- OMIE - ERP Financeiro
- Dynamics 365

## Risco: Senhas fracas

**Criticidade:** Urgente

**Classificação de impacto:** Alto

**Personas afetadas pelo risco:** Não Informado

**Data de registro:** 09/07/2024

**Responsável atual pela gestão do risco:** Anderson Mattiuci

**% de probabilidade de ocorrência:** 80%

**Status atual:** Encontrado

**Data do disparo:** Não Informado

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Recrutamento e Seleção

**Tratamento de dados pessoais associados ao risco:**

- Realizar Recrutamento de seleção

**Ativos da informação associados ao risco:**

- OMIE - ERP Financeiro
- Netsac - CRM
- Dynamics 365

## Risco: Falta de backup automático

**Criticidade:** Alta

**Classificação de impacto:** Alto

**Personas afetadas pelo risco:** Operador

**Data de registro:** 03/06/2024

**Responsável atual pela gestão do risco:** Anderson Mattiuci

**% de probabilidade de ocorrência:** 50%

**Status atual:** Encontrado

**Data do disparo:** Não Informado

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Cadastrar dependentes

**Tratamento de dados pessoais associados ao risco:**

- Cadastrar dependentes

**Ativos da informação associados ao risco:**

- Netsac - CRM

## Risco: Falta de medida técnica

**Criticidade:** Moderada

**Classificação de impacto:** Alto  
**Personas afetadas pelo risco:** Não Informado  
**Data de registro:** 02/08/2024  
**Responsável atual pela gestão do risco:** Anderson Mattiuci

**% de probabilidade de ocorrência:** 10%  
**Status atual:** Encontrado  
**Data do disparo:** Não Informado

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

Dados não cadastrado

#### Risco: Falta de revisão de processos

**Criticidade:** Moderada

**Classificação de impacto:** Alto

**Personas afetadas pelo risco:** Não Informado

**Data de registro:** 01/01/2024

**Responsável atual pela gestão do risco:** Anderson Mattiuci

**% de probabilidade de ocorrência:** 10%

**Status atual:** Disparado

**Data do disparo:** Não Informado

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

Dados não cadastrado

#### Risco: Expiração de senha superior a 90 dias

**Criticidade:** Alta

**Classificação de impacto:** Alto

**Personas afetadas pelo risco:** Titulares

**Data de registro:** 17/07/2024

**Responsável atual pela gestão do risco:** Diego Silva dos Santos

**% de probabilidade de ocorrência:** 50%

**Status atual:** Encontrado

**Data do disparo:** Não Informado

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Contratação CLT

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

- Servidor Local

**Risco:** Risco gerado pelo checklist padrão, através do item (ID): 2

**Criticidade:** Baixa

**Classificação de impacto:** Baixo

**% de probabilidade de ocorrência:** 10%

**Personas afetadas pelo risco:** Não Informado

**Status atual:** Encontrado

**Data de registro:** 11/09/2024

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Anderson Mattiuci

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

Dados não cadastrado

**Risco:** Risco de Due Diligence referente ao fornecedor: Security Max Ltda - CNPJ: 495.000.390-00167

**Criticidade:** Urgente

**Classificação de impacto:** Alto

**% de probabilidade de ocorrência:** 100%

**Personas afetadas pelo risco:** Não Informado

**Status atual:** Encontrado

**Data de registro:** 27/05/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Diego Silva dos Santos

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Reavaliar a empresa analisada.

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

Dados não cadastrado

#### Risco: Período de Retenção Excessivo dos Dados dos Candidatos Não Contratados

**Criticidade:** Moderada

**Classificação de impacto:** Alto

**% de probabilidade de ocorrência:** 10%

**Personas afetadas pelo risco:** Não Informado

**Status atual:** Encontrado

**Data de registro:** 02/06/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Anderson Mattiuci

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Contratação CLT

**Tratamento de dados pessoais associados ao risco:**

- Coletar fotos de candidatos

**Ativos da informação associados ao risco:**

Dados não cadastrado

#### Risco: (Assistant) - Verificar ativo com confiabilidade baixa: Servidor Local

**Criticidade:** Baixa

**Classificação de impacto:** Baixo

**% de probabilidade de ocorrência:** 40%

**Personas afetadas pelo risco:** Não Informado

**Status atual:** Encontrado

**Data de registro:** 09/06/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Diego Silva dos Santos

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Verificar a CID do ativo

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

Dados não cadastrado

### Risco: (Assistant) - Política com vigência expirada: Contratações

**Criticidade:** Urgente

**Classificação de impacto:** Alto

**% de probabilidade de ocorrência:** 100%

**Personas afetadas pelo risco:** Não Informado

**Status atual:** Encontrado

**Data de registro:** 17/07/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Anderson Mattiuci

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Revisar política e estender sua vigência

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

Dados não cadastrado

### Risco: Risco de Due Diligence referente ao fornecedor: People Search Ltda - CNPJ: 263.655.080-00187

**Criticidade:** Baixa

**Classificação de impacto:** Médio

**% de probabilidade de ocorrência:** 10%

**Personas afetadas pelo risco:** Operador

**Status atual:** Controlado

**Data de registro:** 18/07/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Diego Silva dos Santos

### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Reavaliar a empresa analisada.

Ações após disparo:

- Não Informado

### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

Ativos da informação associados ao risco:

Dados não cadastrado

**Risco: Risco de Due Diligence referente ao fornecedor: Lotorian Tecnologia LTDA - CNPJ: 840.332.800-00124**

**Criticidade:** Alta

**Classificação de impacto:** Alto

**% de probabilidade de ocorrência:** 50%

**Personas afetadas pelo risco:** Operador

**Status atual:** Encontrado

**Data de registro:** 22/08/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Adilson Taub Jr

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Reavaliar a empresa analisada.

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Contratação CLT

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

- OMIE - ERP Financeiro

**Risco: Notificação na empresa sobre vazamento de dados**

**Criticidade:** Moderada

**Classificação de impacto:** Alto

**% de probabilidade de ocorrência:** 10%

**Personas afetadas pelo risco:** Não Informado

**Status atual:** Encontrado

**Data de registro:** 04/08/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Anderson Mattiuci

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Não Informado

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Contratação CLT

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

- Servidor Local

**Risco: Risco de Due Diligence referente ao fornecedor: Omnisblue - CNPJ: 290.045.720-00120**

**Criticidade:** Baixa

**Classificação de impacto:** Baixo

**Personas afetadas pelo risco:** Controlador, Titulares

**Data de registro:** 04/09/2025

**Responsável atual pela gestão do risco:** Diego Silva dos Santos

**% de probabilidade de ocorrência:** 50%

**Status atual:** Encontrado

**Data do disparo:** Não Informado

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Aceitar

O que estamos fazendo para tratar o risco:

- Reavaliar a empresa analisada.

Ações após disparo:

- teste 11/09

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Contratação CLT

**Tratamento de dados pessoais associados ao risco:**

**Dados não cadastrado**

**Ativos da informação associados ao risco:**

- OMIE - ERP Financeiro

**Risco: Risco de Due Diligence referente ao fornecedor: People Search Ltda - CNPJ: 263.655.080-00187**

**Criticidade:** Baixa

**Classificação de impacto:** Baixo

**Personas afetadas pelo risco:** Titulares

**Data de registro:** 18/09/2025

**Responsável atual pela gestão do risco:** Diego Silva dos Santos

**% de probabilidade de ocorrência:** 50%

**Status atual:** Disparado

**Data do disparo:** Não Informado

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Reavaliar a empresa analisada.

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Contratação CLT

**Tratamento de dados pessoais associados ao risco:**

**Dados não cadastrado**

**Ativos da informação associados ao risco:**

- Servidor Local

**Risco: Risco de Due Diligence referente ao fornecedor: People Search Ltda - CNPJ: 263.655.080-00187**

**Criticidade:** Moderada

**Classificação de impacto:** Baixo

**Personas afetadas pelo risco:** Operador, Titulares

**% de probabilidade de ocorrência:** 70%

**Status atual:** Encontrado

Data de registro: 22/09/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Diego Silva dos Santos

#### Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- Reavaliar a empresa analisada.

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

Processos de negócios associados ao risco:

- Contratação CLT

Tratamento de dados pessoais associados ao risco:

Dados não cadastrado

Ativos da informação associados ao risco:

Dados não cadastrado

**Risco: Risco de Due Diligence referente ao fornecedor: Matt Consulting - CNPJ: 720.716.880-00101**

Criticidade: Baixa

Classificação de impacto: Médio

% de probabilidade de ocorrência: 10%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 07/10/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Diego Silva dos Santos

#### Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Evitar

O que estamos fazendo para tratar o risco:

- Reavaliar a empresa analisada.

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

Processos de negócios associados ao risco:

Dados não cadastrado

Tratamento de dados pessoais associados ao risco:

Dados não cadastrado

Ativos da informação associados ao risco:

Dados não cadastrado

**Risco: (Assistant) - Verificar ativo com confiabilidade baixa: Dynamics 365**

Criticidade: Urgente

Classificação de impacto: Alto

% de probabilidade de ocorrência: 100%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 22/10/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Anderson Mattiuci

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Verificar a CID do ativo

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

Dados não cadastrado

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

Dados não cadastrado

**Risco: (Assistant) - Contrato com vigência expirada: Certificado Iso**

**Criticidade:** Alta

**Classificação de impacto:** Médio

**% de probabilidade de ocorrência:** 70%

**Personas afetadas pelo risco:** Titulares

**Status atual:** Encontrado

**Data de registro:** 22/10/2025

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Diego Silva dos Santos

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Revisar contrato e extender sua vigência

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

• Contratação CLT

**Tratamento de dados pessoais associados ao risco:**

Dados não cadastrado

**Ativos da informação associados ao risco:**

• Servidor Local

**Risco: Avaliação DDI com alto índice de criticidade Média e Alta**

**Criticidade:** Moderada

**Classificação de impacto:** Médio

**% de probabilidade de ocorrência:** 30%

**Personas afetadas pelo risco:** Controlador

**Status atual:** Encontrado

**Data de registro:** 08/01/2026

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Anderson Mattiuci

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Evitar

O que estamos fazendo para tratar o risco:

- Levantar com o fiscal do contrato o que esta ocorrendo com a prestação de serviço do avaliado.

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

- Cadastrar dependentes
- Contratação Estagiário
- Realizar exames periódicos

**Tratamento de dados pessoais associados ao risco:**

**Dados não cadastrado**

**Ativos da informação associados ao risco:**

**Dados não cadastrado**

**Risco: Ativo sem medidas técnicas atreladas**

**Criticidade:** Moderada

**Classificação de impacto:** Baixo

**% de probabilidade de ocorrência:** 80%

**Personas afetadas pelo risco:** Controlador, Titulares

**Status atual:** Disparado

**Data de registro:** 22/04/2026

**Data do disparo:** Não Informado

**Responsável atual pela gestão do risco:** Anderson Mattiuci

#### Sobre a estratégia de gestão do risco

**Estratégia adotada para tratar o risco:** Mitigar

O que estamos fazendo para tratar o risco:

- Levantamento e implementação de medidas técnicas necessárias.

Ações após disparo:

- Não Informado

#### Sobre as associações do risco

**Processos de negócios associados ao risco:**

**Dados não cadastrado**

**Tratamento de dados pessoais associados ao risco:**

- Cadastrar dependentes

**Ativos da informação associados ao risco:**

- Sistema Legado de Contabilidade
- Servidor Local