EMITIDO EM
05/11/2026 às 16:07:29

Relatório de Impacto à Proteção de Dados Pessoais

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 apectos atuais escopo da Lei Geral de Proteção de Dados.

01 Identificação do controlador

CNPJ
97.676.693/0001-79

WEBSITE
https://www.omnisblue.com

TELEFONE
1146689000

RAZÃO SOCIAL
OMNISBLUE COMPLIANCE SERVICOS E PARTICIPACOES LTDA

ENDEREÇO
Santos

ÁREA DE ATUAÇÃO
Serviço

TIPO DE ATUAÇÃO
Privada

TIPO DE DPO
Interno

DPO RESPONSÁVEL
Adilson Taub Jr

CONTATO DO DPO
adilson.taub@omnisblue.com

02 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	ENCERRAMENTO	RESPONSÁVEL
Não informado	*Não informado*	Adilson Taub Jr

Parâmetros selecionados

Parâmetros selecionados para geração deste DPIA

DIRETORIA	ÁREA	DEPARTAMENTO
Não informado	*Não informado*	*Não informado*
HIPÓTESE	**PAPEL**	**OPERADOR**
Não informado	*Não informado*	*Não informado*
ATIVO	**FINALIDADE**	**SOMENTE ALTO IMPACTO**
Não informado	*Não informado*	Não

03 Tratamento de dados pessoais

A seguir são listados os tratamentos de dados pessoais em execução pelo controlador, hipóteses de tratamento previstas na LGPD, fundamentos legais e ativos de informação utilizados.

Dados não localizados

04 Medidas administrativas de segurança

12 políticas

Medidas administrativas (políticas) em vigor que documentam os compromissos do controlador com a privacidade dos titulares.

Política: Manual de Segurança da Informação

TIPO DA POLÍTICA
Interna

INÍCIO DE VIGÊNCIA	FIM DE VIGÊNCIA
04/05/2026	31/05/2028

RESPONSÁVEL ATUAL PELA POLÍTICA
Adilson Taub Jr

TEM PROCESSO DE MANUTENÇÃO?	TÍTULO DO PROCESSO DE MANUTENÇÃO
Não	*Não informado*

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 DE VIGÊNCIA
30/05/2030

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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 DE VIGÊNCIA
30/05/2029

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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 DE VIGÊNCIA
22/05/2030

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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 DE VIGÊNCIA
22/05/2030

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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 DE VIGÊNCIA
29/05/2030

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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 DE VIGÊNCIA
30/05/2029

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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 DE VIGÊNCIA
23/05/2029

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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 DE VIGÊNCIA
29/05/2030

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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: Direitos dos Titulares de Dados

TIPO DA POLÍTICA
Interna

INÍCIO DE VIGÊNCIA
22/07/2026

FIM DE VIGÊNCIA
27/12/2029

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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: Resposta a incidentes

TIPO DA POLÍTICA
Interna

INÍCIO DE VIGÊNCIA
29/07/2026

FIM DE VIGÊNCIA
29/07/2030

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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: Respostas de Incidentes

TIPO DA POLÍTICA
Publica

INÍCIO DE VIGÊNCIA
11/08/2026

FIM DE VIGÊNCIA
31/08/2027

RESPONSÁVEL ATUAL PELA POLÍTICA
Anderson Mattiuci

TEM PROCESSO DE MANUTENÇÃO?
Não

TÍTULO DO PROCESSO DE MANUTENÇÃO
Não informado

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

05 Medidas técnicas de segurança

10 ativos

Medidas técnicas implementadas em cada ativo utilizado para tratamento de dados pessoais e nível de confiabilidade.

Ativo da informação: OMIE - ERP Financeiro

TIPO
Eletrônico

SUBTIPO
BPMS/Workflow

TECNOLOGIA
Java, Oracle

FORNECEDOR
Não informado

RESPONSÁVEL
Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE

Baixo

CONFIDENCIALIDADE

Baixo

DETALHAMENTO DA CONFIDENCIALIDADE

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

INTEGRIDADE

Baixo

DETALHAMENTO DA INTEGRIDADE

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

DISPONIBILIDADE

Baixo

DETALHAMENTO DA DISPONIBILIDADE

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

Medidas técnicas implementadas

Medida: 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: 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: 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.
Mirror: Cria uma cópia exata dos dados em tempo real, como um espelho.

Medida: 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: 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: Security Robot 2.0

Security Robot 2.0

Riscos associados ao ativo

- 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	SUBTIPO	TECNOLOGIA
Eletrônico	BPMS/Workflow	C#, JavaScript

FORNECEDOR	RESPONSÁVEL
Não informado	Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE

Baixo

CONFIDENCIALIDADE

Baixo

DETALHAMENTO DA CONFIDENCIALIDADE

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

INTEGRIDADE

Baixo

DETALHAMENTO DA INTEGRIDADE

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

DISPONIBILIDADE

Baixo

DETALHAMENTO DA DISPONIBILIDADE

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

Medidas técnicas implementadas

Medida: 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: 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: 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.
Mirror: Cria uma cópia exata dos dados em tempo real, como um espelho.

Medida: 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: 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: Security Robot 2.0

Security Robot 2.0

Medida: 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: 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.

Riscos associados ao ativo

- Senhas fracas
- Falta de backup automático

Ativo da informação: Dynamics 365

TIPO	SUBTIPO	TECNOLOGIA
Eletrônico	BPMS/Workflow	*Não informado*

FORNECEDOR	RESPONSÁVEL
Não informado	Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE

Baixo

CONFIDENCIALIDADE

Baixo

DETALHAMENTO DA CONFIDENCIALIDADE

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

INTEGRIDADE

Baixo

DETALHAMENTO DA INTEGRIDADE

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

DISPONIBILIDADE

Baixo

DETALHAMENTO DA DISPONIBILIDADE

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

Medidas técnicas implementadas

Medida: 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: 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: 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.
Mirror: Cria uma cópia exata dos dados em tempo real, como um espelho.

Medida: 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: 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: Security Robot 2.0

Security Robot 2.0

Medida: Criptografia

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

Medida: 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.

Riscos associados ao ativo

- Senhas fracas
- Acesso indevido ao sistema OMIE

Ativo da informação: Privacy Portal

TIPO	SUBTIPO	TECNOLOGIA
Eletrônico	Plataforma de controle de acesso	Script Case , HTML, AJAX, CSS

FORNECEDOR	RESPONSÁVEL
Não informado	Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE
Alto

CONFIDENCIALIDADE
Médio

DETALHAMENTO DA CONFIDENCIALIDADE
(O Ativo não possui medidas obrigatórias)

INTEGRIDADE
Médio

DETALHAMENTO DA INTEGRIDADE
(O Ativo não possui medidas obrigatórias) Criptografia dos Backups, Redundância dos Backups

DISPONIBILIDADE
Médio

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

Medidas técnicas implementadas

Medida: Security Robot 2.0

Security Robot 2.0

Medida: 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.

Riscos associados ao ativo

Dados não cadastrados

Ativo da informação: System Saúde

TIPO
Eletrônico

SUBTIPO
BPMS/Workflow

TECNOLOGIA
Não informado

FORNECEDOR
Não informado

RESPONSÁVEL
Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE

Não informado

CONFIDENCIALIDADE

Médio

DETALHAMENTO DA CONFIDENCIALIDADE

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.

INTEGRIDADE

Médio

DETALHAMENTO DA INTEGRIDADE

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.

DISPONIBILIDADE

Médio

DETALHAMENTO DA DISPONIBILIDADE

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.

Medidas técnicas implementadas

Medida: Security Robot 2.0

Security Robot 2.0

Riscos associados ao ativo

- Falta de política de privacidade

Ativo da informação: Dynamics Sales

TIPO

Eletrônico

SUBTIPO

ERP

TECNOLOGIA

MS Dynamics 365

FORNECEDOR

People Search Ltda

RESPONSÁVEL

Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE

Médio

CONFIDENCIALIDADE

Alto

DETALHAMENTO DA CONFIDENCIALIDADE

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

INTEGRIDADE

Médio

DETALHAMENTO DA INTEGRIDADE

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

DISPONIBILIDADE

Médio

DETALHAMENTO DA DISPONIBILIDADE

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

Medidas técnicas implementadas

Medida: Medida técnica da Excelsior

Não informado

Medida: Security Robot 2.0

Security Robot 2.0

Medida: 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: 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: Criptografia dos Backups

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

Medida: Recaptha

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

Medida: 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: 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: 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: 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: 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: 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: 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: 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: Gestão e contole de versões

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

Medida: Treinamento de Segurança para Funcionários

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

Medida: 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: 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: 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: 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.

Riscos associados ao ativo

Dados não cadastrados

Ativo da informação: Servidor Local

TIPO
Eletrônico

SUBTIPO
Servidor de arquivo

TECNOLOGIA
Não informado

FORNECEDOR
TECH Talent informatica Ltda

RESPONSÁVEL
Jonas Evangelista da Silva

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE
Médio

CONFIDENCIALIDADE
Alto

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

INTEGRIDADE
Alto

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

DISPONIBILIDADE
Médio

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

Medidas técnicas implementadas

Medida: 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: 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: Criptografia dos Backups

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

Medida: 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: Recaptha

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

Medida: 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: 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: 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: 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: 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: Atualizações e Patches

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

Medida: Treinamento de Segurança para Funcionários

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

Medida: 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: 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: 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: 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.

Riscos associados ao ativo

- Notificação na empresa sobre vazamento de dados
- Risco de Due Diligence referente ao fornecedor: People Search Ltda - CNPJ: 263.655.080-00187
- Expiração de senha superior a 90 dias
- Ativo sem medidas técnicas atreladas

Ativo da informação: Sistema Legado de Folha de Pagamento

TIPO	SUBTIPO	TECNOLOGIA
Eletrônico	ERP	*Não informado*

FORNECEDOR	RESPONSÁVEL
Não informado	Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE

Alto

CONFIDENCIALIDADE

Alto

DETALHAMENTO DA CONFIDENCIALIDADE

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

INTEGRIDADE

Alto

DETALHAMENTO DA INTEGRIDADE

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

DISPONIBILIDADE

Alto

DETALHAMENTO DA DISPONIBILIDADE

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

Medidas técnicas implementadas

Medida: 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: 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: 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: 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: Recaptha

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

Medida: 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: 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: 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: 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: Atualizações e Patches

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

Medida: 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: 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: 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: Criptografia dos Backups

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

Medida: 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: 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: 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: 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: 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: Gestão e contole de versões

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

Riscos associados ao ativo

Dados não cadastrados

Ativo da informação: Sistema Legado de Contabilidade

TIPO
Eletrônico

SUBTIPO
Não informado

TECNOLOGIA
Cobol , Banco de Dados DB2,

FORNECEDOR
Amaratuns Consultoria Ltda

RESPONSÁVEL
Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE
Baixo

CONFIDENCIALIDADE
Baixo

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

INTEGRIDADE
Baixo

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

DISPONIBILIDADE
Baixo

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

Medidas técnicas implementadas

Medida: 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: Gestão e contole de versões

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

Medida: 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.

Riscos associados ao ativo

- Ativo sem medidas técnicas atreladas
- Acessos indevidos - Sistema Contábil legado

Ativo da informação: CAD People

TIPO
Eletrônico

SUBTIPO
Não informado

TECNOLOGIA
C++

FORNECEDOR
TECH Talent informatica Ltda

RESPONSÁVEL
Anderson Mattiuci

Nível de confiabilidade

NÍVEL GERAL DE CONFIABILIDADE
Baixo

CONFIDENCIALIDADE
Médio

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

INTEGRIDADE
Médio

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

DISPONIBILIDADE
Baixo

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

Medidas técnicas implementadas

Medida: Recaptha

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

Medida: 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: 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: 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: 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: Treinamento de Segurança para Funcionários

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

Medida: 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: 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: 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: 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.

Riscos associados ao ativo

- Falta de matriz de acesso
- Vazamenteo de dados de dependentes VIP

06 Gestão de riscos de privacidade e segurança da informação

30 riscos

Para a gestão de riscos de privacidade e segurança da informação, utilizamos a seguinte matriz estruturada para classificação da criticidade de cada risco, composta de acordo com a classificação de impacto e sua probabilidade percentual de ocorrência.

PROBABILIDADE	IMPACTO: BAIXO	IMPACTO: MÉDIA	IMPACTO: ALTO
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

Riscos de privacidade identificados e gerenciados pelo controlador, ordenados por criticidade.

Risco: Acesso indevido ao sistema OMIE

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Alta	Médio	80%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Titulares	04/08/2024	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Mitigar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Ativar MFA obrigatório no Omie.
Segmentar perfis por função, revogando acessos amplos.
Desativar contas no offboarding imediatamente.
Revisar logs de acesso mensalmente.

AÇÕES APÓS DISPARO
Bloqueio e Contenção Imediata: Revogar a sessão ativa, alterar credenciais e desativar o usuário comprometido no painel do Omie.
Avaliação de Impacto e Logs: Extrair o log de auditoria para mapear dados visualizados, editados ou exportados (clientes, financeiro, fiscal).
Erradicação: Inspecionar integrações via API vinculadas à conta, rotacionar chaves/tokens de aplicação e validar integridade dos registros.
Comunicação e Conformidade: Acionar o DPO/Comitê de Crise para avaliar risco relevante aos titulares e eventual notificação à autoridade competente.
Pós-Incidente: Identificar o vetor de entrada (phishing, credencial vazada, ausência de MFA) e aplicar medidas corretivas para evitar reincidência.

Associações do risco

PROCESSOS DE NEGÓCIO
- Cadastrar dependentes
- Recrutamento e Seleção

FINALIDADES DE TRATAMENTO
- Cadastrar dependentes
- Realizar Recrutamento de seleção

ATIVOS DE INFORMAÇÃO
- OMIE - ERP Financeiro
- Dynamics 365

Risco: Senhas fracas

CRITICIDADE
Urgente

IMPACTO
Alto

PROBABILIDADE
80%

STATUS
Encontrado

PERSONAS AFETADAS
Não informado

DATA REGISTRO
09/07/2024

DATA DISPARO
Não informado

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Recrutamento e Seleção

FINALIDADES DE TRATAMENTO
- Realizar Recrutamento de seleção

ATIVOS DE INFORMAÇÃO
- OMIE - ERP Financeiro
- Netsac - CRM
- Dynamics 365

Risco: Falta de backup automático

CRITICIDADE
Alta

IMPACTO
Alto

PROBABILIDADE
50%

STATUS
Encontrado

PERSONAS AFETADAS
Operador

DATA REGISTRO
03/06/2024

DATA DISPARO
Não informado

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Cadastrar dependentes

FINALIDADES DE TRATAMENTO
- Cadastrar dependentes

ATIVOS DE INFORMAÇÃO
- Netsac - CRM

Risco: Falta de medida técnica

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Moderada	Alto	10%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	02/08/2024	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
Dados não cadastrados

Risco: Falta de revisão de processos

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Moderada	Alto	10%	Disparado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	01/01/2024	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
Dados não cadastrados

Risco: Expiração de senha superior a 90 dias

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Alta	Alto	50%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Titulares	17/07/2024	*Não informado*

RESPONSÁVEL
Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Contratação CLT

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
- Servidor Local

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

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Baixa	Baixo	10%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	11/09/2024	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

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

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Urgente	Alto	100%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	27/05/2025	*Não informado*

RESPONSÁVEL
Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA
Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Reavaliar a empresa analisada.

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO

Dados não cadastrados

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

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

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Moderada	Alto	10%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	02/06/2025	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Contratação CLT

FINALIDADES DE TRATAMENTO
- Coletar fotos de candidatos

ATIVOS DE INFORMAÇÃO
Dados não cadastrados

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

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Baixa	Médio	10%	Controlado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Operador	18/07/2025	*Não informado*

RESPONSÁVEL
Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Reavaliar a empresa analisada.

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

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

CRITICIDADE
Alta

IMPACTO
Alto

PROBABILIDADE
50%

STATUS
Encontrado

PERSONAS AFETADAS
Operador

DATA REGISTRO
22/08/2025

DATA DISPARO
Não informado

RESPONSÁVEL
Adilson Taub Jr

Estratégia de gestão

ESTRATÉGIA ADOTADA
Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Reavaliar a empresa analisada.

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Contratação CLT

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO
- OMIE - ERP Financeiro

Risco: Notificação na empresa sobre vazamento de dados

CRITICIDADE
Moderada

IMPACTO
Alto

PROBABILIDADE
10%

STATUS
Encontrado

PERSONAS AFETADAS
Não informado

DATA REGISTRO
04/08/2025

DATA DISPARO
Não informado

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Contratação CLT

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
- Servidor Local

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

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Baixa	Baixo	50%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Controlador,Titulares	04/09/2025	*Não informado*

RESPONSÁVEL
Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Reavaliar a empresa analisada.

AÇÕES APÓS DISPARO
teste 11/09

Associações do risco

PROCESSOS DE NEGÓCIO
- Contratação CLT

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
- OMIE - ERP Financeiro

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

CRITICIDADE
Baixa

IMPACTO
Baixo

PROBABILIDADE
50%

STATUS
Disparado

PERSONAS AFETADAS
Titulares

DATA REGISTRO
18/09/2025

DATA DISPARO
Não informado

RESPONSÁVEL
Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA
Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Reavaliar a empresa analisada.

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Contratação CLT

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
- Servidor Local

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

CRITICIDADE
Moderada

IMPACTO
Baixo

PROBABILIDADE
70%

STATUS
Encontrado

PERSONAS AFETADAS
Operador,Titulares

DATA REGISTRO
22/09/2025

DATA DISPARO
Não informado

RESPONSÁVEL
Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA
Mitigar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Reavaliar a empresa analisada.

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
- Contratação CLT

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
Dados não cadastrados

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

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Baixa	Médio	10%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	07/10/2025	*Não informado*

RESPONSÁVEL
Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA
Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Reavaliar a empresa analisada.

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

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

CRITICIDADE
Moderada

IMPACTO
Médio

PROBABILIDADE
30%

STATUS
Encontrado

PERSONAS AFETADAS
Controlador

DATA REGISTRO
08/01/2026

DATA DISPARO
Não informado

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
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

Associações do risco

PROCESSOS DE NEGÓCIO
- Cadastrar dependentes
- Contratação Estagiário

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

Risco: Ativo sem medidas técnicas atreladas

CRITICIDADE
Moderada

IMPACTO
Baixo

PROBABILIDADE
80%

STATUS
Disparado

PERSONAS AFETADAS
Controlador,Titulares

DATA REGISTRO
22/04/2026

DATA DISPARO
Não informado

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA

Mitigar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO

Levantamento e implementação de medidas técnicas necessárias.

AÇÕES APÓS DISPARO

Não informado

Associações do risco

PROCESSOS DE NEGÓCIO

Dados não cadastrados

FINALIDADES DE TRATAMENTO

- Cadastrar dependentes

ATIVOS DE INFORMAÇÃO

- Sistema Legado de Contabilidade
- Servidor Local

Risco: Falta de compartilhamento de politicas e códigos com colaboradores

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Alta	Alto	40%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	21/05/2026	*Não informado*

RESPONSÁVEL

Diego Silva dos Santos

Estratégia de gestão

ESTRATÉGIA ADOTADA

Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO

Não informado

AÇÕES APÓS DISPARO

Não informado

Associações do risco

PROCESSOS DE NEGÓCIO

- Contratação CLT

FINALIDADES DE TRATAMENTO

- Cadastrar colaboradores (CLT)

ATIVOS DE INFORMAÇÃO

- Armario Físico de pastas de clientes

Risco: Acessos indevidos - Sistema Contábil legado

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Moderada	Médio	40%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Operador,Controlador,Titulares	02/06/2026	*Não informado*

RESPONSÁVEL

Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA

Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO

Para mitigar o risco de acessos indevidos em um sistema contábil legado, a estratégia deve ser dividida entre contenção imediata (curto prazo) e sustentação de longo prazo, visto que sistemas legados frequentemente impedem a implementação nativa de tecnologias modernas.

Aqui está uma estratégia estruturada:

Estratégia de Mitigação: Proteção de Ativo Legado
1. Camada de Acesso (Contenção Imediata)
Como o sistema legado pode não suportar integrações modernas, o foco é cercar a aplicação sem alterá-la.

Virtualização de Acesso (Jump Server): O acesso ao sistema não deve ser feito diretamente pelas estações de trabalho. Utilize um Jump Server (servidor de salto) onde o acesso seja controlado via MFA (Autenticação de Múltiplos Fatores). O usuário entra no Jump Server com seu ID corporativo (ex: AD/Azure) e, apenas lá, executa o software legado.

Segmentação de Rede (Micro-segmentação): Mova o sistema para uma sub-rede isolada (VLAN) que só permita conexões vindas do Jump Server ou de IPs específicos autorizados, bloqueando qualquer comunicação externa (Internet) ou lateral (dentro da rede local).

2. Gestão de Identidades e Privilégios (Governança)
Desprovisionamento Automático: Sincronize a base de usuários do sistema legado com o RH. Sempre que um colaborador for desligado no sistema central, uma tarefa automatizada (via script SQL ou RPA) deve desativar ou remover o usuário no banco de dados do sistema legado.

Privilégio Mínimo (Hardening): Elimine usuários com privilégios de "Administrador" ou "Superusuário". Utilize perfis operacionais estritos e, para tarefas administrativas, utilize uma conta de serviço com senha complexa armazenada em um Cofre de Senhas (ex: CyberArk, Bitwarden, HashiCorp).

3. Monitoramento e Detecção (Visibilidade)
Auditoria de Logs: Se o sistema não gera logs de acesso nativos, implemente uma auditoria no nível do Banco de Dados. Configure triggers (gatilhos) que registrem toda tentativa de SELECT, UPDATE ou DELETE em tabelas contábeis sensíveis em uma tabela de log separada.

SIEM/Alertas: Exporte esses logs para uma ferramenta de monitoramento. Crie alertas para comportamentos anômalos, como:

Acesso fora do horário comercial.

Múltiplas tentativas de login falhas.

Consultas massivas de dados (exportações).

4. Ciclo de Vida (Visão Estratégica)
Shadowing (Espelhamento): Se o sistema precisa ser mantido por questões fiscais, realize uma migração da base para um repositório moderno (ReadOnly). O sistema legado original deve ser mantido "offline" ou em modo "arquivamento", acessível apenas mediante processo formal.

Plano de Descontinuação: Estabeleça uma data limite para o encerramento da dependência deste software. Sem um horizonte de desativação, o risco nunca é eliminado, apenas gerenciado.

AÇÕES APÓS DISPARO

Plano de Ação: Proteção e Gestão de Sistema Contábil Legado
Fase 1: Estabilização e Controle (Semanas 1-2)
Foco: Reduzir a superfície de ataque imediata.

Inventário de Acessos: Realizar um dump de todos os usuários ativos no banco de dados do sistema legado.

Limpeza de Contas (Cleanup):

Excluir ou desativar contas de ex-colaboradores (contas órfãs).

Identificar usuários com privilégio de "Administrador" e restringir ao mínimo necessário.

Segregação Inicial: Configurar regra no firewall para que o servidor do sistema legado aceite conexões apenas dos IPs das estações de trabalho autorizadas (bloqueio de acesso via rede Wi-Fi comum ou visitantes).

Fase 2: Fortalecimento da Camada de Acesso (Semanas 3-6)
Foco: Implementar o controle de acesso intermediado.

Configuração do Jump Server:

Preparar um ambiente (VM) dedicado para acesso ao legado.

Integrar o login deste ambiente ao Active Directory (AD) com MFA obrigatório.

Políticas de Senha: Forçar a alteração de todas as senhas de acesso ao legado, exigindo complexidade (seguindo a política de segurança da empresa).

Treinamento: Instruir a equipe contábil sobre o novo fluxo de trabalho (Acesso via Jump Server).

Fase 3: Monitoramento e Auditoria (Semanas 7-10)
Foco: Visibilidade para detecção de incidentes.

Implementação de Triggers de Auditoria:

Criar rotinas de banco de dados para registrar alterações em tabelas críticas (Ex: logs de UPDATE/DELETE em tabelas de lançamentos contábeis).

Centralização de Logs: Definir um local seguro (fora do servidor do sistema) onde esses logs serão armazenados e protegidos contra alteração (Write Once, Read Many - WORM, se possível).

Testes de Intrusão (Simulado): Executar um teste para verificar se o monitoramento dispara alertas quando um acesso não autorizado é tentado fora do fluxo do Jump Server.

Fase 4: Governança e Descontinuidade (Contínuo)
Foco: Manutenção e visão de futuro.

Revisão Mensal: Incluir na pauta da equipe de TI/Compliance a revisão dos acessos ao sistema legado.

Estudo de Viabilidade (RPA/Migração): Iniciar a documentação funcional do que é indispensável no legado para balizar a futura migração ou a extração de dados para um Data Warehouse seguro.

Associações do risco

PROCESSOS DE NEGÓCIO
- Geração de DCTF

FINALIDADES DE TRATAMENTO
- Gerar DCTF

ATIVOS DE INFORMAÇÃO
- Sistema Legado de Contabilidade

Risco: Avaliação com criticidade urgente

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Urgente	Alto	80%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	20/07/2026	*Não informado*

RESPONSÁVEL
Mike Ross

Estratégia de gestão

ESTRATÉGIA ADOTADA
Mitigar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Verificar com o RH o entendimento mais profundo dos conflitos identificados

AÇÕES APÓS DISPARO
Informar o gestor imediato.
Informar o RH.
Chamar comitê para providências.

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
Dados não cadastrados

Risco: Stresse por atividade de alta complexidade - Fechamento de Folha mensal

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Alta	Médio	50%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	01/07/2026	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Acompanhar o fechamento de folha pelo RH.

AÇÕES APÓS DISPARO
Encaminhar os analistas de folha para avaliação do RH

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
Dados não cadastrados

Risco: Atestado de saúde com indicação de burnout

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Moderada	Alto	10%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	30/07/2026	*Não informado*

RESPONSÁVEL
Anderson Mattiuci da Silva

Estratégia de gestão

ESTRATÉGIA ADOTADA

Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO

Enviar para tratemento

AÇÕES APÓS DISPARO

Não informado

Associações do risco

PROCESSOS DE NEGÓCIO

Dados não cadastrados

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

Risco: Falta de matriz de acesso

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Alta	Alto	60%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Controlador	18/08/2026	*Não informado*

RESPONSÁVEL

Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA

Mitigar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO

Estabelecer, implementar e monitorar um modelo de Controle de Acesso Baseado em Funções (RBAC) para garantir que os usuários tenham apenas o nível mínimo de acesso necessário para exercerem suas atividades (Princípio do Menor Privilégio).

Mapeamento e Levantamento de Funções

Realizar entrevistas com os gestores das áreas que utilizam o CAD People (ex: RH, DP, TI, Gestores) para entender as necessidades reais de acesso de cada cargo.

Identificar os dados sensíveis armazenados no sistema e quem estritamente precisa visualizá-los ou editá-los.

Desenho da Matriz de Acesso (RBAC)

Criar um documento formal cruzando os Perfis de Usuário (ex: Analista de RH, Coordenador, Suporte TI, Leitura-Gestor) com as Funcionalidades/Telas do sistema.

Aplicar a regra de Segregação de Funções (SoD - Segregation of Duties), garantindo que nenhum usuário tenha permissões conflitantes (ex: aprovar a própria alteração cadastral).

Implementação Técnica no Sistema

Configurar os perfis desenhados na matriz dentro do ambiente do CAD People.

Bloquear acessos diretos a banco de dados ou funcionalidades administrativas para usuários não autorizados.

Saneamento e Migração de Acessos (Clean-up)

Mapear todos os usuários ativos atualmente no sistema.

Enquadrar os usuários existentes nos novos perfis criados.

Revogar imediatamente todos os acessos genéricos, compartilhados ou excessivos (contas super-admin em posse de usuários comuns).

Formalização do Processo de Concessão (JML)

Criar um fluxo documentado para entrada (Joiner), movimentação (Mover) e desligamento (Leaver) de colaboradores, atrelando a liberação de acesso no CAD People à aprovação formal do gestor direto e do dono do sistema.

AÇÕES APÓS DISPARO

1. Contenção Imediata (Estancar o Impacto)
O objetivo principal é interromper a ação não autorizada imediatamente para evitar maiores danos.

Bloqueio Preventivo: Congelar ou suspender temporariamente a conta do usuário ou usuários envolvidos na violação.

Rebaixamento de Privilégios (Downgrade): Caso o bloqueio total inviabilize a operação crítica da empresa, alterar temporariamente o perfil do usuário para "Somente Leitura" até que a situação seja esclarecida.

Isolamento do Sistema: Em casos de comprometimento massivo (ex: uso de uma conta super-administrador genérica vazada), desativar temporariamente a integração do CAD People com outros sistemas (como o sistema de folha ou ERP) para evitar a propagação do dano.

2. Investigação e Análise de Impacto
Identificar a extensão do problema sem alterar os vestígios.

Extração de Logs: Coletar e preservar os logs de auditoria do CAD People correspondentes ao período do incidente (quem acessou, de qual IP, que horas e qual alteração foi feita).

Avaliação de LGPD: Verificar se foram acessados, alterados ou exportados dados pessoais sensíveis dos colaboradores (salários, atestados médicos, dados bancários).

Levantamento de Danos: Confirmar se houve impacto financeiro (ex: alteração de conta bancária para recebimento de salário) ou impacto operacional.

3. Remediação e Recuperação
Corrigir os danos causados pela falha de acesso.

Restauração de Dados (Rollback): Reverter as alterações indevidas no banco de dados do CAD People utilizando backups ou trilhas de auditoria válidas.

Revogação Definitiva: Excluir permanentemente as permissões que permitiram o incidente, garantindo que o usuário tenha seu acesso restrito à sua função atual.

Aceleração da Mitigação: Tratar a implementação imediata de uma Matriz de Acesso básica (mesmo que simplificada) como prioridade máxima ("War Room").

4. Comunicação e Compliance
Assegurar a transparência e cumprir requisitos legais.

Acionamento do DPO: Envolver imediatamente o Encarregado de Proteção de Dados (DPO) e o Jurídico caso haja violação de dados pessoais.

Notificação de Partes Interessadas: Comunicar os gestores das áreas afetadas e, se exigido pela legislação (ANPD), notificar os titulares dos dados afetados pelo vazamento/incidente.

Associações do risco

PROCESSOS DE NEGÓCIO

Dados não cadastrados

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO

- CAD People

Risco: Fornecedor com muitas mídias negativas

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Baixa	Baixo	40%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Controlador	18/09/2026	*Não informado*

RESPONSÁVEL

Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA

Evitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO

Rever o contrato

AÇÕES APÓS DISPARO

Comunicar o conselho deliberativo

Associações do risco

PROCESSOS DE NEGÓCIO

Dados não cadastrados

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

Risco: Fluxo de dados sensíveis em modelos de IA

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Alta	Médio	70%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Controlador	23/09/2026	*Não informado*

RESPONSÁVEL
Anderson Mattiuci da Silva

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
Dados não cadastrados

Risco: Vazamenteo de dados de dependentes VIP

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Moderada	Alto	10%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Operador,Controlador,Titulares	06/10/2026	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO
Dados não cadastrados

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO
- CAD People

Risco: Processo de compras de serviço tecnológico

CRITICIDADE	IMPACTO	PROBABILIDADE	STATUS
Alta	Médio	60%	Encontrado

PERSONAS AFETADAS	DATA REGISTRO	DATA DISPARO
Não informado	13/10/2026	*Não informado*

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Comunicar a diretoria de compras

Associações do risco

PROCESSOS DE NEGÓCIO
- Realizar compras de itens de tecnologia

FINALIDADES DE TRATAMENTO
Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

Risco: Postura incorreta em atividades com notebook

CRITICIDADE
Moderada

IMPACTO
Alto

PROBABILIDADE
10%

STATUS
Encontrado

PERSONAS AFETADAS
Não informado

DATA REGISTRO
12/10/2026

DATA DISPARO
Não informado

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA
Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO
Não informado

AÇÕES APÓS DISPARO
Não informado

Associações do risco

PROCESSOS DE NEGÓCIO

Dados não cadastrados

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados

Risco: Descargas elétricas

CRITICIDADE
Moderada

IMPACTO
Alto

PROBABILIDADE
10%

STATUS
Encontrado

PERSONAS AFETADAS
Não informado

DATA REGISTRO
14/10/2026

DATA DISPARO
Não informado

RESPONSÁVEL
Anderson Mattiuci

Estratégia de gestão

ESTRATÉGIA ADOTADA

Aceitar

O QUE ESTAMOS FAZENDO PARA TRATAR O RISCO

Não informado

AÇÕES APÓS DISPARO

Não informado

Associações do risco

PROCESSOS DE NEGÓCIO

Dados não cadastrados

FINALIDADES DE TRATAMENTO

Dados não cadastrados

ATIVOS DE INFORMAÇÃO

Dados não cadastrados