RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Emitido em: 13/03/2025 às 11:45:30

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.

Identificação do controlador

CNPJ: 97.676.693/0001-79

Razão Social: OMNISBLUE COMPLIANCE SERVICOS E PARTICIPACOES LTDA (Apresentação)

Endereço: Santos

Website: https://www.omnisblue.com

Área de atuação: Serviço

Tipo de atuação: Privada

Tipo de DPO: Interno

DPO Resposável: Adilson Taub Jr

Contato do DPO: 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

Diretoria: Não informado
Área: Não informado
Departamento: Não informado
Hipótese: Não informado
Papel: Não informado
Operador: Não informado
Ativo: Não informado
Finalidade: Não informado

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: Realizar Recrutamento de seleção

Hipótese de tratamento (LGPD): Art. 11º, II a - Obrigação legal ou regulatória
Papel da entidade: Controlador
Trata dados sensíveis? Sim
Trata dados de crianças/adolescentes?: Não
Origem da Informação: Candidato
Destino da Informação: RH
Frequência: Baixa (mensalmente)
Volumetria: Alto (1000 - 10000)

Fundamentos Legais

Dados não cadastrado

Sobre os dados em tratamento

Artefatos: Certidão de Casamento
Lista de dados pessoais tratados na finalidade:

- Data | do casamento | Cadastral | Imprescindível para o tratamento? Sim
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Sim
- Nome | do cônjuge | Cadastral | Imprescindível para o tratamento? Sim

Artefatos: Certidão de Nascimento
Lista de dados pessoais tratados na finalidade:

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

Artefatos: Registro Geral (RG)
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 | RG | Cadastral | Imprescindível para o tratamento? Sim
- Orgão | expeditor | Cadastral | Imprescindível para o tratamento? Sim

Artefatos: Relatório - Exame admissional
Lista de dados pessoais tratados na finalidade:

- Alergias | Sem especialização | Dado Sensível de Saúde | Imprescindível para o tratamento? Não
- DNA | Sem especialização | Biométrico Sensível | Imprescindível para o tratamento? Não
- Doenças | Sem especialização | Dado Sensível de Saúde | Imprescindível para o tratamento? Não
- Iris | Sem especialização | Biométrico Sensível | Imprescindível para o tratamento? Não
- Tipo Sanguíneo | Sem especialização | Dado Sensível de Saúde | Imprescindível para o tratamento? Não

Sobre o processo de consentimento

O tratamento depende de consentimento: Não

Sobre operadores associados

Utiliza Operador? Sim **Operador:** People Search Ltda
Contrato: Contratação de colaboradores
Início da Vigência: 01/01/2024 **Fim da Vigência:** 31/12/2024

Sobre o compartilhamento de informações

Os dados são compartilhados? Sim

Como os dados são compartilhados: Não Informado

Com quem os dados são compartilhados
Dados não cadastrados

Realiza transferências internacionais ? Sim
Com quais países os dados são compartilhados?

- Bélgica
- Bermuda

Sobre o fim do tratamento dos dados

Os dados são descartados? Sim **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: OMIE - ERP Financeiro **Tipo:** Eletrônico

Título do ativo: System Saúde **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: Senhas fracas

Título do risco: Acesso indevido ao sistema OMIE

Finalidade: Cadastrar dependentes

Hipótese de tratamento (LGPD): Art. 11º, II a - Obrigação legal ou regulatória

Papel da entidade: Controlador

Trata dados sensíveis? Sim

Trata dados de crianças/adolescentes?: Sim

Origem da Informação: Colaborador

Destino da Informação: RH

Frequência: Baixa (mensalmente)

Volumetria: Médio (500 - 999)

Fundamentos Legais

Consolidação das Leis do Trabalho (CLT)

Sobre os dados em tratamento

Artefatos: Certidão de Casamento

Lista de dados pessoais tratados na finalidade:

- Data | do casamento | Cadastral | Imprescindível para o tratamento? Sim
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Sim
- Nome | do cônjuge | Cadastral | Imprescindível para o tratamento? Sim

Artefatos: Certidão de Nascimento

Lista de dados pessoais tratados na finalidade:

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

Sobre o processo de consentimento

O tratamento depende de consentimento: Não

Sobre operadores associados

Dados não cadastrado

Sobre o compartilhamento de informações

Os dados são compartilhados? Sim

Como os dados são compartilhados: Não Informado

Com quem os dados são compartilhados
Dados não cadastrados

Realiza transferências internacionais ? Não Informado

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: OMIE - ERP Financeiro **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: Acesso indevido ao sistema OMIE

Finalidade: Coletar fotos de candidatos

Hipótese de tratamento (LGPD): Art. 7º, I - Consentimento do Titular

Papel da entidade: Controlador

Trata dados sensíveis? Não

Trata dados de crianças/adolescentes?: Não

Origem da Informação: Candidato

Destino da Informação: RH

Frequência: Média (semanalmente)

Volumetria: Médio (500 - 999)

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

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 Informado

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:

Dados não cadastrado

Finalidade: Envio de convites para eventos

Hipótese de tratamento (LGPD): Art. 7º, IX - Legítimo interesse do controlador

Papel da entidade: Controlador

Trata dados sensíveis? Não

Trata dados de crianças/adolescentes?: Não

Origem da Informação: Clientes e Parceiros

Destino da Informação: Marketing

Frequência: Média (semanalmente)

Volumetria: Baixo (100 - 499)

Fundamentos Legais

Dados não cadastrado

Sobre os dados em tratamento

Artefatos: CPF

Lista de dados pessoais tratados na finalidade:

- Data | de emissão | Cadastral | Imprescindível para o tratamento? Não

- Nome | do portador | Cadastral | Imprescindível para o tratamento? Não
- Número | do CPF | Cadastral | Imprescindível para o tratamento? Não

Artefatos: Registro Geral (RG)
Lista de dados pessoais tratados na finalidade:

- Data | de emissão | Cadastral | Imprescindível para o tratamento? Não
- Nome | do portador | Cadastral | Imprescindível para o tratamento? Não
- Número | RG | Cadastral | Imprescindível para o tratamento? Não
- Orgão | expeditor | Cadastral | Imprescindível para o tratamento? Não

Sobre o processo de consentimento

O tratamento depende de consentimento: Não

Sobre operadores associados

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

Título do ativo: OMIE - ERP Financeiro **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

Finalidade: Atender aos direitos do Titular de dados

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

Fundamentos Legais

Art. 18. da Lei 13.709/18

Sobre os dados em tratamento

Artefatos: Certidão de Nascimento
Lista de dados pessoais tratados na finalidade:

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

Artefatos: Contrato de Trabalho
Lista de dados pessoais tratados na finalidade:

- CEP | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Data | da contratação | Cadastral | Imprescindível para o tratamento? Não
- Gênero | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Nome | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Plano de saúde | Sem especialização | Dado Sensível de Saúde | Imprescindível para o tratamento? Não
- Profissão | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Tipo Sanguíneo | Sem especialização | Dado Sensível de Saúde | Imprescindível para o tratamento? Não

Sobre o processo de consentimento

O tratamento depende de consentimento: Não

Sobre operadores associados

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: Política de Privacidade

Tipo da política: Publica
Início de vigência: 01/01/2018 **Fim da vigência:** 31/12/2050
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: Política de Cookies

Tipo da política: Publica
Início de vigência: 01/01/2018 **Fim da vigência:** 31/12/2050
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

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

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. Mirror: 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

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: Criptografia

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

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. Mirror: 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

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: Alto

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- Não Informado

Nível de Integridade das informações tratadas pelo ativo: Alto

- Não Informado

Nível de Disponibilidade das informações tratadas pelo ativo: Alto

- 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: Criptografia

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

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. Mirror: 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

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

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: Sistema Excelsior

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 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 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.

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: Não Informado

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

% de probabilidade de ocorrência: 80%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 09/07/2024

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:
• 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

% de probabilidade de ocorrência: 50%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 03/06/2024

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:
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 medida técnica

Criticidade: Moderada

Classificação de impacto: Alto
% de probabilidade de ocorrência: 10%
Personas afetadas pelo risco: Não Informado
Status atual: Encontrado
Data de registro: 02/08/2024
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:
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
% de probabilidade de ocorrência: 10%
Personas afetadas pelo risco: Não Informado
Status atual: Disparado
Data de registro: 01/01/2024
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:
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: Moderada
Classificação de impacto: Alto
% de probabilidade de ocorrência: 10%
Personas afetadas pelo risco: Não Informado
Status atual: Encontrado
Data de registro: 17/07/2024
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:
Dados não cadastrado

Tratamento de dados pessoais associados ao risco:
Dados não cadastrado

Ativos da informação associados ao risco:
Dados não cadastrado

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