RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Emitido em: 30/05/2025 às 11:22:58

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

Identificação do controlador

CNPJ: 62.014.352/0002-34

Razão Social: ASSOCIAÇÃO ESCOLA SUIÇO-BRASILEIRA - Curitiba

Endereço: Wanda dos Santos Mallmann

Website: https://chpr.aesb.com.br/

Área de atuação: Serviço

Tipo de atuação: Economia Mista

Tipo de DPO: Externo

DPO Externo: Omnisblue Compliance Serviços e Participações LTDA.

Responsável do DPO Externo: Adilson Taub Jr.

Tel. Responsável DPO Externo: Não Informado

E-mail Responsável DPO Externo: 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: 06/09/2024	**Encerramento:** Não Informado	**Responsável:** Adilson Taub Jr.
Etapa de Adequação:		
Início: 06/09/2024	**Encerramento:** Não Informado	**Responsável:** Adilson Taub Jr.
Etapa de Operação:		
Início: 06/09/2024	**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:** Coletar ou atualizar biometria

Tratamento de dados pessoais

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

Finalidade: Coletar ou atualizar biometria

Hipótese de tratamento (LGPD): Art. 11º, II g - Prev. à fraude no cadastro de sist. elet.

Papel da entidade: Controlador

Trata dados sensíveis? Sim

Trata dados de crianças/adolescentes?: Sim

Origem da Informação: Titular de dados

Destino da Informação: Portaria e recepção (Sistema Secullum)

Frequência: Alta (diariamente)

Volumetria: Baixo (100 - 499)

Fundamentos Legais

Dados não cadastrado

Sobre os dados em tratamento

Artefatos: Cadastro / Atualização do usuário

Lista de dados pessoais tratados na finalidade:

- Biometria facial | do colaborador | Biométrico Sensível | Imprescindível para o tratamento? Sim
- Biometria facial | do pai do aluno | Biométrico Sensível | Imprescindível para o tratamento? Sim
- Biometria facial | da mãe do aluno | Biométrico Sensível | Imprescindível para o tratamento? Sim
- Biometria facial | do aluno | Biométrico Sensível | Imprescindível para o tratamento? Sim
- Biometria facial | do terceiro | Biométrico Sensível | Imprescindível para o tratamento? Sim
- Data | de nascimento do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Data | de nascimento do pai do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Data | de nascimento da mãe do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Data | de nascimento do colaborador | Biográfico | Imprescindível para o tratamento? Sim
- Data | de nascimento do terceiro | Biográfico | Imprescindível para o tratamento? Sim
- E-mail | do terceiro | Biográfico | Imprescindível para o tratamento? Sim
- E-mail | do colaborador | Biográfico | Imprescindível para o tratamento? Sim

- E-mail | da mãe do aluno | Biográfico | Imprescindível para o tratamento? Sim
- E-mail | do pai do aluno | Biográfico | Imprescindível para o tratamento? Sim
- E-mail | do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Endereço físico | do terceiro | Biográfico | Imprescindível para o tratamento? Sim
- Endereço físico | do colaborador | Biográfico | Imprescindível para o tratamento? Sim
- Endereço físico | da mãe do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Endereço físico | do pai do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Endereço físico | do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Nome | do terceiro | Biográfico | Imprescindível para o tratamento? Sim
- Nome | do colaborador | Biográfico | Imprescindível para o tratamento? Sim
- Nome | da mãe do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Nome | do pai do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Nome | do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Número de telefone | do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Número de telefone | do pai do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Número de telefone | da mãe do aluno | Biográfico | Imprescindível para o tratamento? Sim
- Número de telefone | do colaborador | Biográfico | Imprescindível para o tratamento? Sim
- Número de telefone | do terceiro | Biográfico | Imprescindível para o tratamento? Sim
- Número do CPF | do aluno | Cadastral | Imprescindível para o tratamento? Sim
- Número do CPF | do pai do aluno | Cadastral | Imprescindível para o tratamento? Sim
- Número do CPF | da mãe do aluno | Cadastral | Imprescindível para o tratamento? Sim
- Número do CPF | do colaborador | Cadastral | Imprescindível para o tratamento? Sim
- Número do CPF | do terceiro | Cadastral | Imprescindível para o tratamento? Sim
- Número do RG | da mãe do aluno | Cadastral | Imprescindível para o tratamento? Sim
- Número do RG | do aluno | Cadastral | Imprescindível para o tratamento? Sim
- Número do RG | do pai do aluno | Cadastral | Imprescindível para o tratamento? Sim
- Número do RG | do colaborador | Cadastral | Imprescindível para o tratamento? Sim
- Número do RG | do terceiro | 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? 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: Secullum - Sistema de gerenciamento de acesso **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: Vazamento ou acesso não autorizado aos dados pessoais biométrico

Título do risco: Oposição ao tratamento de dados biométricos de controle de acesso

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: 01/11/2024 **Fim da vigência:** 30/11/2026
Responsável atual pela política: Luiz Gustavo Ortigara
Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Sim **Está completa?** Sim **É exequível?** Sim
Trata o papel do Titular? Sim **Trata o papel do DPO?** Sim **Trata Operadores?** Sim

Abrange o processo de gestão de riscos? Sim
Abrange o processo de gestão de incidentes? Sim
Abrange compartilhamento de dados pessoais? Sim

Política: Política de Cookies

Tipo da política: Publica
Início de vigência: 26/05/2025 **Fim da vigência:** 26/05/2027
Responsável atual pela política: Luiz Gustavo Ortigara
Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Sim **Está completa?** Sim **É exequível?** Sim
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: Aviso de Privacidade – Tratamento de Dados Biométricos para Controle de Acesso

Tipo da política: Publica
Início de vigência: 01/06/2025 **Fim da vigência:** 01/06/2027
Responsável atual pela política: Luiz Gustavo Ortigara
Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Sim **Está completa?** Sim **É exequível?** Sim
Trata o papel do Titular? Sim **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: Privacy Portal (PP)

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS – PHP com MySQL Server **Fornecedor atual:** Omnisblue Compliance Serviços e Participações LTDA.

Responsável atual pela gestão do ativo: Daniel Zaitz

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Alto

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- Para avaliar a confidencialidade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Nível de Integridade das informações tratadas pelo ativo: Alto

- Para avaliar a integridade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Nível de Disponibilidade das informações tratadas pelo ativo: Alto

- Para avaliar a disponibilidade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Sobre as medidas técnicas de segurança implementadas no ativo

Medida técnica: Firewall

Os ativos associados a esta medida estão protegidos com um firewall WAF (Web Application Firewall) que protege contra ameaças e ataques direcionados a essas aplicações web.

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: 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: 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: 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: Logs de acesso

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

Medida técnica: Criptografia de Dados em Repouso

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

Medida técnica: 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: 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: Implementação de soluções de redundância para componentes críticos (servidores, redes, armazenamento).
Duplicar componentes críticos da infraestrutura para garantir a disponibilidade dos serviços em caso de falha de um dos componentes (servidores, redes, armazenamento).

Medida técnica: Atualizações e Patches
Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas operacionais.

Medida técnica: Atualizações e Patches
Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas operacionais.

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

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

Medida técnica: Recuperação de acessos
Trata-se das rotinas de recuperação de acessos a ativos que porventura tenham sido perdidos por usuários.

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: Privacy & Compliance Project (PCP)

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS – PHP com MySQL Server **Fornecedor atual:** Omnisblue Compliance Serviços e Participações LTDA.

Responsável atual pela gestão do ativo: Daniel Zaitz

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Alto

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- Para avaliar a confidencialidade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Nível de Integridade das informações tratadas pelo ativo: Alto

- Para avaliar a integridade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Nível de Disponibilidade das informações tratadas pelo ativo: Alto

- Para avaliar a disponibilidade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Sobre as medidas técnicas de segurança implementadas no ativo

Medida técnica: Firewall
Os ativos associados a esta medida estão protegidos com um firewall WAF (Web Application Firewall) que protege contra ameaças e ataques direcionados a essas aplicações web.

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

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

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

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

Medida técnica: 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: 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: Implementação de soluções de redundância para componentes críticos (servidores, redes, armazenamento).
Duplicar componentes críticos da infraestrutura para garantir a disponibilidade dos serviços em caso de falha de um dos componentes (servidores, redes, armazenamento).

Medida técnica: Atualizações e Patches
Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas

operacionais.

Medida técnica: Atualizações e Patches
Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas operacionais.

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

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

Medida técnica: Recuperação de acessos
Trata-se das rotinas de recuperação de acessos a ativos que porventura tenham sido perdidos por usuários.

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: Privacy Action (PAC)

Tipo do ativo: Eletrônico
Subtipo: Sistema de gestão
Tecnologia envolvida: SaaS – PHP com MySQL Server
Fornecedor atual: Omnisblue Compliance Serviços e Participações LTDA.
Responsável atual pela gestão do ativo: Daniel Zaitz

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Alto

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- Para avaliar a confidencialidade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Nível de Integridade das informações tratadas pelo ativo: Alto

- Para avaliar a integridade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Nível de Disponibilidade das informações tratadas pelo ativo: Alto

- Para avaliar a disponibilidade de um ativo, é fundamental considerar uma série de critérios baseados na ISO 27001 e no NIST, que garantam a proteção dos dados contra acessos não autorizados e vazamentos. Neste caso, a nota foi considerada alta porque a maioria das medidas técnicas obrigatórias e recomendadas para este ativo foram rigorosamente atendidas.

Sobre as medidas técnicas de segurança implementadas no ativo

Medida técnica: Firewall
Os ativos associados a esta medida estão protegidos com um firewall WAF (Web Application Firewall) que protege contra ameaças e ataques direcionados a essas aplicações web.

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: 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: Listas de controle de acesso (ACLs)

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

Medida técnica: Recaptha

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

Medida técnica: 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: Logs de acesso

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

Medida técnica: Criptografia de Dados em Repouso

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

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

Duplicar componentes críticos da infraestrutura para garantir a disponibilidade dos serviços em caso de falha de um dos componentes (servidores, redes, armazenamento).

Medida técnica: Atualizações e Patches

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

Medida técnica: Atualizações e Patches

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

Medida técnica: Análise de Vulnerabilidades

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

Medida técnica: Análise de Vulnerabilidades

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

Medida técnica: Recuperação de acessos

Trata-se das rotinas de recuperação de acessos a ativos que porventura tenham sido perdidos por usuários.

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: SUPER (SEI ANPD)

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS **Fornecedor atual:** Autoridade Nacional de Proteção de Dados (ANPD)

Responsável atual pela gestão do ativo: Daniel Zaitz

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 é gerenciado pelo controlador, e, portanto, tanto a análise como a garantia de atendimento às melhores práticas de confidencialidade estão sob o escopo de atuação do terceiro que mantém o ativo.

Nível de Integridade das informações tratadas pelo ativo: Médio

- o O ativo não é gerenciado pelo controlador, e, portanto, tanto a análise como a garantia de atendimento às melhores práticas de integridade estão sob o escopo de atuação do terceiro que mantém o ativo.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- o O ativo não é gerenciado pelo controlador, e, portanto, tanto a análise como a garantia de atendimento às melhores práticas de disponibilidade estão sob o escopo de atuação do terceiro que mantém o ativo.

Sobre as medidas técnicas de segurança implementadas no ativo

Dados não cadastrado

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: Site ESB de Cutirtiba

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: IaaS **Fornecedor atual:** TS PECORARI NETWORKS E TECNOLOGIA DA INFOR

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Alto

Nível de Confidencialidade das informações tratadas pelo ativo: Alto

- A confidencialidade do sistema é alta, pois todas as medidas necessárias estão em vigor. O controle de acesso baseado em funções (RBAC) garante que os usuários tenham acesso restrito às informações de acordo com suas funções e responsabilidades. Logs de acesso são registrados e monitorados, garantindo rastreabilidade e segurança das informações. A criptografia de dados em trânsito é aplicada para proteger as informações durante a comunicação, prevenindo interceptações e vazamentos. Ferramentas de DPL (Data Loss Prevention) estão implementadas para realizar a verificação contínua da integridade dos dados armazenados, evitando perda ou acesso não autorizado a dados sensíveis. A aplicação

regular de atualizações e patches de segurança mantém todos os sistemas e softwares protegidos contra vulnerabilidades conhecidas. Programas de treinamento regulares conscientizam os funcionários sobre práticas seguras e políticas de segurança, garantindo que todos estejam preparados para manter a confidencialidade das informações. Além disso, foi criado um Plano de Recuperação de Desastre de TI (DRP), com procedimentos definidos para responder a eventos catastróficos que possam impactar os sistemas de TI. A implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças assegura que qualquer falha seja rapidamente identificada e tratada, garantindo a continuidade dos serviços e a proteção dos dados.

Nível de Integridade das informações tratadas pelo ativo: Alto

- A integridade do sistema é alta, pois a maioria das medidas necessárias está implementada. Realizam-se backups regulares, com recuperação testada periodicamente, garantindo que falhas possam ser revertidas rapidamente. O controle de acesso baseado em funções (RBAC) e logs de acesso garantem que apenas usuários autorizados possam alterar os dados. A criptografia de dados em trânsito protege as informações durante a comunicação, enquanto ferramentas de DPL (Data Loss Prevention) monitoram a integridade dos dados armazenados. A aplicação regular de atualizações e patches de segurança mantém todos os sistemas protegidos contra vulnerabilidades. Programas de treinamento conscientizam os funcionários sobre práticas seguras, e o Plano de Recuperação de Desastre de TI (DRP) define procedimentos claros para eventos catastróficos. Processos eficazes de detecção e gerenciamento de incidentes garantem a rápida resposta a falhas, mantendo a integridade dos dados.

Nível de Disponibilidade das informações tratadas pelo ativo: Alto

- A disponibilidade do sistema é alta, pois todas as medidas necessárias estão implementadas para garantir que os serviços estejam sempre acessíveis e operacionais. Realizam-se backups regulares, com recuperação testada periodicamente, garantindo que dados possam ser restaurados rapidamente em caso de falha. A implementação de ferramentas de DPL (Data Loss Prevention) assegura que a integridade dos dados armazenados seja constantemente monitorada, evitando perda ou corrupção. A aplicação regular de atualizações e patches de segurança mantém os sistemas protegidos, e programas de treinamento são realizados para conscientizar os funcionários sobre práticas seguras e políticas de segurança. Foi criado um Plano de Recuperação de Desastre de TI (DRP) com procedimentos bem definidos para responder a eventos catastróficos que possam afetar a operação dos sistemas de TI. A definição de SLAs claros garante o cumprimento de métricas específicas de disponibilidade e tempo de resposta, enquanto processos eficazes de detecção e gerenciamento de incidentes asseguram uma resposta rápida a falhas, garantindo a continuidade do serviço.

Sobre as medidas técnicas de segurança implementadas no ativo

Medida técnica: Backups Regulares e Recuperação dos Backups
Consiste em copiar os dados importantes para um local seguro (físico ou na nuvem) em intervalos regulares. A recuperação de backups permite restaurar os dados em caso de perda, corrupção ou desastres.

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

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

Medida técnica: 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: 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: 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: Logs de acesso

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

Medida técnica: 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: 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: Atualizações e Patches

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

Medida técnica: Atualizações e Patches

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

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: 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: Ferramentas de detecção de falhas

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

Medida técnica: Ferramentas de detecção de falhas

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

Medida técnica: Criptografia dos Backups

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

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: 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: Redundância dos Backups

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

Medida técnica: Autenticação multifator (MFA)

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

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

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

Medida técnica: 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: 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: Implementação de soluções de redundância para componentes críticos (servidores, redes, armazenamento).
Duplicar componentes críticos da infraestrutura para garantir a disponibilidade dos serviços em caso de falha de um dos componentes (servidores, redes, armazenamento).

Medida técnica: Configuração de mecanismos de failover automatizado para garantir a continuidade do serviço em caso de falhas.
Implementar sistemas que automaticamente direcionam o tráfego para um sistema redundante em caso de falha do sistema principal, minimizando o tempo de inatividade.

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

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

Medida técnica: 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: Treinamento de Segurança para Funcionários
Educar os funcionários sobre as melhores práticas de segurança da informação, como senhas fortes, phishing, engenharia social, etc.

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

Medida técnica: Contratos de Nível de Serviço (SLAs)
Acordos entre o provedor de serviços e o cliente que definem os níveis de serviço esperados, incluindo tempo de resposta a incidentes de segurança, tempo de inatividade permitido, etc.

Medida técnica: Contratos de Nível de Serviço (SLAs)
Acordos entre o provedor de serviços e o cliente que definem os níveis de serviço esperados, incluindo tempo de resposta a

incidentes de segurança, tempo de inatividade permitido, etc.

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

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

Medida técnica: Gerenciamento de Incidentes e ameaças
Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

Sobre os riscos associados

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

Dados não cadastrado

Ativo da informação: Servidor de E-mail

Tipo do ativo: Eletrônico **Subtipo:** Plataforma de e-mail

Tecnologia envolvida: SaaS **Fornecedor atual:** GOOGLE BRASIL INTERNET LTDA.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Sistema de arquivos (Google Workspace)

Tipo do ativo: Eletrônico **Subtipo:** Servidor de arquivo

Tecnologia envolvida: SaaS **Fornecedor atual:** GOOGLE BRASIL INTERNET LTDA.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Sistema de assinatura digital (TOTVS)

Tipo do ativo: Eletrônico **Subtipo:** Outro

Tecnologia envolvida: SaaS **Fornecedor atual:** TOTVS S.A.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Google Drive

Tipo do ativo: Eletrônico **Subtipo:** Servidor de arquivo

Tecnologia envolvida: SaaS **Fornecedor atual:** GOOGLE BRASIL INTERNET LTDA.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Linkedin

Tipo do ativo: Eletrônico **Subtipo:** Outro

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** MICROSOFT INFORMATICA LTDA

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Whatsapp

Tipo do ativo: Eletrônico **Subtipo:** Mensageria eletrônica

Tecnologia envolvida: SaaS mobile **Fornecedor atual:** Facebook Servicos Online do Brasil Ltda.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: TOTVS

Tipo do ativo: Eletrônico **Subtipo:** ERP

Tecnologia envolvida: SaaS **Fornecedor atual:** TOTVS S.A.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Plataforma CIEE

Tipo do ativo: Eletrônico **Subtipo:** Outro

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** Centro de Integração Empresa-Escola do Paraná

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: eSocial

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** Receita Federal Ministério da Fazenda

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Banco Itaú

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: Portal web SaaS **Fornecedor atual:** Itaú Unibanco Holding S.A.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Plataforma Ativamed(site)

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** Ativamed Medicina e Segurança do Trabalho Ltda.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Plataforma(site) - Metrocard

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** Associação Metrocard

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Plataforma VEM São José(site)

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** Consórcio Vem São José

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Plataforma TICKET(site)

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** Ticket Serviços S.A

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Plataforma VT Urbs(site)

Tipo do ativo: Eletrônico **Subtipo:** Portal corporativo

Tecnologia envolvida: Portal Web SaaS **Fornecedor atual:** URBS Urbanização de Curitiba S/A

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: eProtocolo

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS **Fornecedor atual:** SERVICO FEDERAL DE PROCESSAMENTO DE DADO

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Educasenso

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS **Fornecedor atual:** INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS E

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Marfin

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS **Fornecedor atual:** SECRETARIA DE ESTADO DA EDUCACAO - SEED

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Layers (aplicativo)

Tipo do ativo: Eletrônico **Subtipo:** Outro

Tecnologia envolvida: SaaS Mobile **Fornecedor atual:** LAYERS LTDA

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Google Meet

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS **Fornecedor atual:** GOOGLE BRASIL INTERNET LTDA.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Google Agenda

Tipo do ativo: Eletrônico **Subtipo:** Sistema de gestão

Tecnologia envolvida: SaaS **Fornecedor atual:** GOOGLE BRASIL INTERNET LTDA.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

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 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

Dados não cadastrado

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: Linha Telefônica

Tipo do ativo: Eletrônico **Subtipo:** Outro

Tecnologia envolvida: Telefonia **Fornecedor atual:** LIGGA TELECOMUNICACOES S.A.

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- Quando uma linha telefônica, fornecida por uma empresa terceirizada, é utilizada em um ramal corporativo, a confidencialidade dos dados torna-se uma preocupação essencial. É imperativo garantir que todas as comunicações realizadas por meio dessa linha sejam protegidas contra acessos não autorizados. Para isso, é fundamental implementar medidas de segurança robustas, como criptografia de ponta a ponta e restrições de acesso baseadas em autorização. Além disso, treinamentos regulares sobre práticas seguras de comunicação e a conscientização sobre a importância da confidencialidade dos dados são essenciais para todos os usuários do ramal. Ao adotar essas precauções, a empresa pode proteger suas informações sensíveis e preservar a confiança de seus clientes e parceiros comerciais.

Nível de Integridade das informações tratadas pelo ativo: Médio

- Quando uma linha telefônica, disponibilizada por uma empresa terceirizada, é utilizada em um ramal corporativo, a integridade dos dados é uma consideração crucial. É essencial garantir que todas as comunicações feitas por meio dessa linha permaneçam íntegras e livres de alterações não autorizadas. Para isso, é importante implementar medidas de segurança, como protocolos de autenticação robustos e criptografia de ponta a ponta. Além disso, realizar verificações regulares de integridade dos dados e monitorar atividades suspeitas ajudam a detectar e mitigar qualquer tentativa de comprometimento. Ao adotar essas precauções, a empresa pode proteger a integridade de suas comunicações e garantir a confiabilidade das informações transmitidas por meio do ramal telefônico.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- Quando uma linha telefônica, fornecida por uma empresa terceirizada, é utilizada em um ramal corporativo, a disponibilidade dos dados é fundamental para garantir a continuidade das comunicações. É crucial que a linha telefônica esteja sempre disponível para uso, sem interrupções que possam afetar as operações comerciais. Para assegurar isso, é importante contar com contratos de serviço robustos com a empresa fornecedora, que incluam garantias de disponibilidade e suporte técnico adequado. Além disso, investir em redundância de rede e sistemas de backup pode ajudar a mitigar possíveis falhas e garantir a disponibilidade contínua das comunicações. Ao adotar essas medidas, a empresa pode manter a disponibilidade dos dados e assegurar que as comunicações via linha telefônica permaneçam ininterruptas, apoiando assim suas operações comerciais.

Sobre as medidas técnicas de segurança implementadas no ativo

Dados não cadastrado

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: Secullum - Sistema de gerenciamento de acesso

Tipo do ativo: Eletrônico **Subtipo:** Plataforma de controle de acesso

Tecnologia envolvida: On-Premise **Fornecedor atual:** TECNOPONTO TECNOLOGIA AVANCADA EM CONTR

Responsável atual pela gestão do ativo: Luiz Gustavo Ortigara

Sobre o nível de confiabilidade do ativo

Nível geral de Confiabilidade do Ativo: Médio

Nível de Confidencialidade das informações tratadas pelo ativo: Médio

- A confidencialidade do Secullum - sistema de gerenciamento de acesso foi classificada como MÉDIA, pois conta com medidas técnicas obrigatórias como Controle de Acesso Baseado em Funções (RBAC), logs de acesso, criptografia de dados em trânsito, atualizações e patches, treinamento de segurança para funcionários, plano de recuperação de desastres e gerenciamento de incidentes e ameaças, garantindo um nível razoável de proteção contra acessos não autorizados. O sistema ainda não conta com medidas técnicas desejáveis, o que limita o seu potencial de avanço para um nível mais elevado de confidencialidade. A ausência de medidas técnicas obrigatórias como DLP (Data Loss Prevention) impactou negativamente a nota, limitando a confidencialidade do sistema. Além disso, a falta de medidas técnicas desejáveis como análise de vulnerabilidades, Recaptcha, listas de controle de acesso (ACLs), autenticação multifator (MFA), criptografia de dados em repouso, gerenciamento de chaves criptográficas e criptografia dos backups poderia contribuir para um nível mais elevado de confidencialidade, garantindo maior proteção do sistema. A implementação dessas medidas é essencial para reforçar a segurança do sistema e garantir maior proteção contra acessos indevidos e vazamentos de informações sensíveis.

Nível de Integridade das informações tratadas pelo ativo: Médio

- A integridade do Secullum - sistema de gerenciamento de acesso foi classificada como MÉDIA, pois conta com medidas técnicas obrigatórias como backups regulares e recuperação dos backups, controle de acesso baseado em funções (RBAC), logs de acesso, criptografia de dados em trânsito, atualizações e patches, treinamento de segurança para funcionários, plano de recuperação de desastres e gerenciamento de incidentes e ameaças, garantindo um nível razoável de segurança dos dados contra alterações indevidas ou acidentais. Além disso, o sistema também possui medidas técnicas desejáveis como soluções de redundância para componentes críticos, mecanismos de failover automatizado e logs de auditoria detalhados, o que aumenta a confiabilidade e resiliência da operação. A ausência de medidas técnicas obrigatórias como testes regulares de recuperação dos backups e DLP (Data Loss Prevention) impactou negativamente a nota, limitando a integridade do sistema. Além disso, a falta de medidas técnicas desejáveis como criptografia dos backups, listas de controle de acesso (ACLs), autenticação multifator (MFA), Recaptcha, ferramentas de detecção de falhas, criptografia de dados em repouso, gerenciamento de chaves criptográficas, gestão e controle de versões e análise de vulnerabilidades poderia contribuir para um nível mais elevado de integridade, garantindo maior confiabilidade do sistema. A implementação dessas medidas é essencial para reforçar a resiliência do sistema e garantir a confiabilidade dos dados mesmo em situações adversas ou ataques maliciosos.

Nível de Disponibilidade das informações tratadas pelo ativo: Médio

- A disponibilidade do Secullum - sistema de gerenciamento de acesso foi classificada como MÉDIA, pois conta com medidas técnicas obrigatórias como backups regulares e recuperação dos backups, redundância dos backups, treinamento de segurança para funcionários, atualizações e patches, plano de recuperação de desastres e gerenciamento de incidentes e ameaças, garantindo um nível razoável de continuidade operacional. Além disso, o sistema também possui medidas técnicas desejáveis como soluções de redundância para componentes críticos e mecanismos de failover automatizado, o que melhora a resiliência da infraestrutura em caso de falhas, reforçando a capacidade de recuperação. A ausência de medidas técnicas obrigatórias como testes regulares de recuperação dos backups e contratos de nível de serviço (SLAs) impactou negativamente a nota, limitando a disponibilidade do sistema. Além disso, a falta de medidas técnicas desejáveis como criptografia dos backups, monitoramento contínuo com alertas em tempo real, ferramentas de detecção de falhas, DLP (Data Loss Prevention), balanceamento de carga e análise de vulnerabilidades poderia contribuir para um nível mais elevado de disponibilidade, garantindo maior resiliência do sistema. A implementação dessas medidas é essencial para consolidar a disponibilidade do sistema e garantir continuidade operacional mesmo diante de eventos críticos ou falhas técnicas.

Sobre as medidas técnicas de segurança implementadas no ativo

Medida técnica: Backups Regulares e Recuperação dos Backups

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

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

Medida técnica: 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: 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: Implementação de soluções de redundância para componentes críticos (servidores, redes, armazenamento).
Duplicar componentes críticos da infraestrutura para garantir a disponibilidade dos serviços em caso de falha de um dos componentes (servidores, redes, armazenamento).

Medida técnica: Configuração de mecanismos de failover automatizado para garantir a continuidade do serviço em caso de falhas.
Implementar sistemas que automaticamente direcionam o tráfego para um sistema redundante em caso de falha do sistema principal, minimizando o tempo de inatividade.

Medida técnica: Atualizações e Patches
Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas operacionais.

Medida técnica: Atualizações e Patches
Aplicar regularmente atualizações de segurança e patches para corrigir vulnerabilidades conhecidas em softwares e sistemas operacionais.

Medida técnica: Treinamento de Segurança para Funcionários
Educar os funcionários sobre as melhores práticas de segurança da informação, como senhas fortes, phishing, engenharia social, etc.

Medida técnica: 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: Gerenciamento de Incidentes e ameaças
Definir procedimentos para lidar com incidentes de segurança, desde a detecção até a resolução, incluindo a comunicação com as partes interessadas e a análise forense.

Sobre os riscos associados

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

- Vazamento ou acesso não autorizado aos dados pessoais biométrico
- Dificuldades de acesso à escola por indisponibilidade do controle de acesso automatizado

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: Vazamento ou acesso não autorizado aos dados pessoais biométrico

Criticidade: Moderada

Classificação de impacto: Alto

% de probabilidade de ocorrência: 20%

Personas afetadas pelo risco: Controlador,Titulares

Status atual: Encontrado

Data de registro: 29/05/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Luiz Gustavo Ortigara

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- Garantir o monitoramento contínuo dos aspectos de segurança dos sistemas envolvidos com o uso de dados biométricos, e executar um processo de gestão de incidentes formal, sempre que ocorrer algum incidente. Implementar outras medidas técnicas de segurança, visando maximizar os níveis de confiabilidade da informação dos sistemas envolvidos com o uso de dados biométricos, em especial: - Testes regulares de recuperação dos backups, mitigando eventuais problemas de perda de dados; - Autenticação multifator (MFA) no sistema de cadastro dos dados, maximizando o nível e confidencialidade das informações; - Monitoria em tempo real dos aspectos de infraestrutura do sistema, diminuindo o lead timing da gestão de eventuais incidentes; - Gestão de controle de versões do sistema, melhorando a capacidade de auditoria em caso de investigações de incidentes; - Implementação de PENTESTs regulares, aumentando o nível de confiabilidade dos ativos e minimizando as chances de acessos externos indevidos aos dados.

Ações após disparo:

- Realizar a imediata suspensão de todos os acessos ao sistema afetado, com a retirada do ambiente do ar (modo offline), visando interromper o impacto, proteger os dados sensíveis e evitar a propagação de eventuais falhas ou ameaças.

Sobre as associações do risco

Processos de negócios associados ao risco:

• RS - Controle de acesso (Catracas)

Tratamento de dados pessoais associados ao risco:

• Coletar ou atualizar biometria

• Controlar acesso as dependências da escola

Ativos da informação associados ao risco:
• Secullum - Sistema de gerenciamento de acesso

Risco: Oposição ao tratamento de dados biométricos de controle de acesso

Criticidade: Baixa
Classificação de impacto: Médio
% de probabilidade de ocorrência: 20%
Personas afetadas pelo risco: Controlador,Titulares
Status atual: Encontrado
Data de registro: 29/05/2025
Data do disparo: Não Informado
Responsável atual pela gestão do risco: Luiz Gustavo Ortigara

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- Manter atualizado o Aviso de Privacidade associado ao tratamento de dados e distribuí-lo amplamente, de forma que fique claro e transparente os detalhes do tratamento dos dados biométricos, enfatizando as finalidades, as medidas de segurança adotadas e as bases legais que autorizam seu uso no controle de acesso. Promover ações de comunicação e orientação para todos os pais e responsáveis, e demais titulares de dados, ressaltando a importância da coleta biométrica para garantir a segurança, a identificação precisa de todos, além da eficiência na gestão do ambiente escolar. Essa abordagem educativa visa minimizar dúvidas, incentivar a colaboração e reduzir a recusa no fornecimento dos dados, assegurando o pleno funcionamento do sistema e a proteção de toda a comunidade escolar.

Ações após disparo:

- Disponibilizar um meio alternativo seguro e eficaz, como a leitura da carteirinha escolar ou a conferência de documentos oficiais, para que o aluno, seus pais ou responsáveis (e demais titulares) possam acessar o ambiente escolar. Essa medida garante a continuidade do controle de acesso e preserva a segurança, sendo adotada imediatamente diante da recusa na coleta biométrica, evitando transtornos e possibilitando o diálogo para esclarecimentos e resolução do impasse.

Sobre as associações do risco

Processos de negócios associados ao risco:
• RS - Controle de acesso (Catracas)

Tratamento de dados pessoais associados ao risco:
• Coletar ou atualizar biometria

• Controlar acesso as dependências da escola

Ativos da informação associados ao risco:
Dados não cadastrado

Risco: Dificuldades de acesso à escola por indisponibilidade do controle de acesso automatizado

Criticidade: Baixa
Classificação de impacto: Baixo
% de probabilidade de ocorrência: 20%
Personas afetadas pelo risco: Controlador,Titulares
Status atual: Encontrado
Data de registro: 30/05/2025
Data do disparo: Não Informado
Responsável atual pela gestão do risco: Luiz Gustavo Ortigara

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- Monitorar os níveis de DISPONIBILIDADE dos sistemas responsáveis pela automação do controle de entrada e saída das escolas e buscar alternativas para garantir o espelhamento da solução.

Ações após disparo:

- Controlar, manualmente, o registro de entrada e saída da escola, evitando filas e garantindo o registro dessas atividades em outros sistemas, mesmo que gerenciados por ativos físicos. Realizar a importação dos dados quando o sistema voltar a estar

disponível, para centralização do histórico.

Sobre as associações do risco

Processos de negócios associados ao risco:
• RS - Controle de acesso (Catracas)

Tratamento de dados pessoais associados ao risco:
Dados não cadastrado

Ativos da informação associados ao risco:
• Secullum - Sistema de gerenciamento de acesso