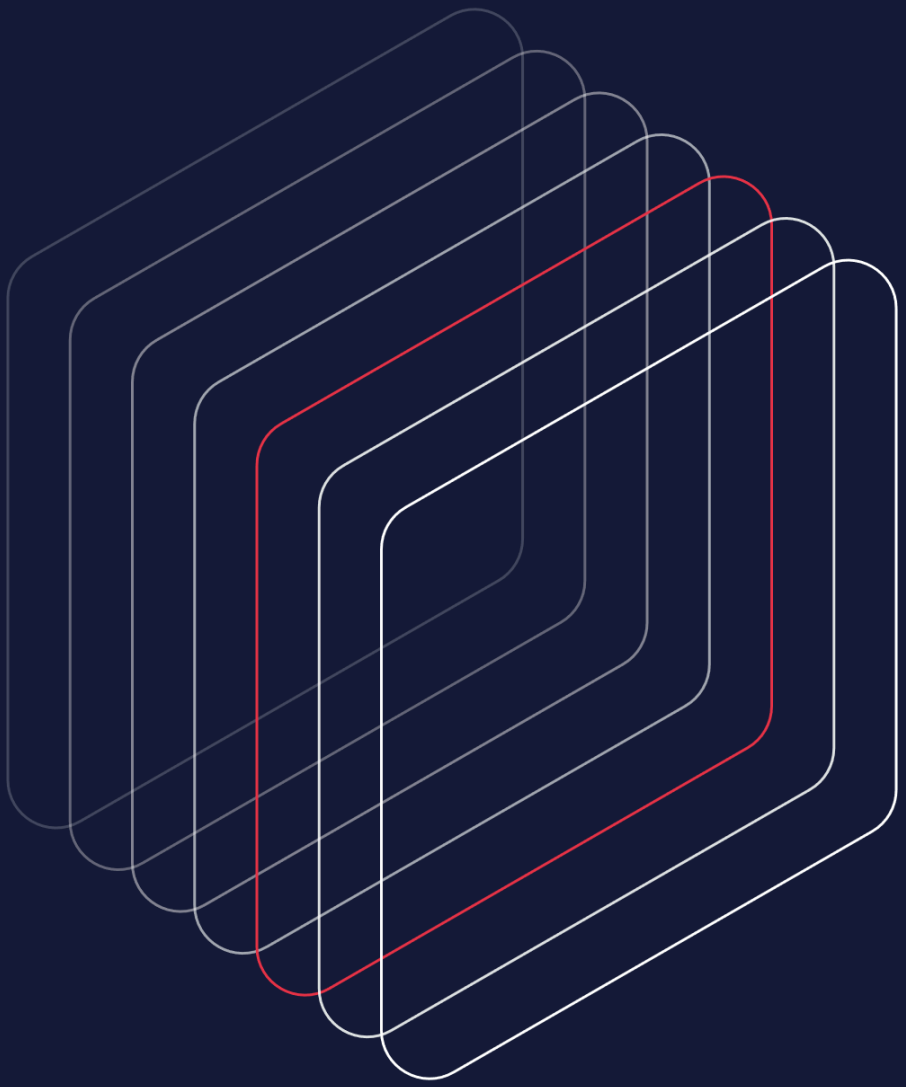

blwinner
Certification Consulting

RELATÓRIO DE CONFORMIDADE ISO/IEC 27017 E 27018

- **DATA ELABORAÇÃO: 12/11/2024**
- **REVISÃO: 01**

- **EMPRESA:**

- **ENDEREÇO:**

End.:	Rua Maria Gonçalves Alexandre 161 Bairro: Cajuru. Sala Esc b1 andar 1. Condomínio ▪ Luiz Franca B CD Com.		
CEP:	82940-420		
Cidade:	Curitiba	**Estado:**	Paraná
CNPJ:	32.545.408/0001-35		
Tel.:	(41) 3359-3600		

QUEM SOMOS?

Somos uma empresa especialista em consultorias, auditorias e treinamentos baseados em Sistemas de Gestão da Qualidade, Meio Ambiente, Saúde e Segurança no Trabalho, Segurança de alimentos e outros.

Atuamos desde 2006 em todo o território nacional, onde já assessoramos mais de 330 empresas, de diferentes segmentos e portes, na adequação das práticas de gestão baseadas pelas normas internacionais ISO 9001, ISO 14001, ISO 45001, SASSMAQ, ISO 20000, ISO 27001, ISO 27701, ISO 37001, ISO 37301 e ISO 39001.

Entendemos que cada empresa é única e justamente por esse motivo, prestamos nossos serviços de forma personalizada, contribuindo para o desenvolvimento da organização antes, durante e depois da obtenção das certificações.

Afinal, a sua qualidade é a nossa maior conquista.

ALGUNS CLIENTES

1. INFORMAÇÕES ADICIONAIS

Razão Social: SAT - SOLUÇÕES EM TECNOLOGIA
CNPJ: 32.545.408/0001-35
Endereço Principal: R. Maria Gonçalves Alexandre, 161 - Bairro: Cajuru. Sala Escb1 andar 1. Condomínio Luiz Franca B CD Com., Curitiba - PR, 82940-420
Emissão do Relatório: 12/11/2024
Contato Cliente: Alan de Carlo Maggi
Telefone: (41) 3359-3600
E-mail: alan.maggi@satsolucoes.com.br

2. ESCOPO DA EMPRESA

Desenvolvimento, implementação e manutenção de soluções tecnológicas e consultivas para a gestão de ativos (EAM) e gestão de manutenção, incluindo os produtos SAT Tracking, SAT Cronos, SAT Planning e SAT Tools, voltados para os setores ferroviário, metroviário, hidroviário, mineração, portuário, energia, florestal, saúde e industrial, em todas as localidades que estão em conformidade com as nossas regulamentações de proteção de dados aplicáveis.

3. CONFIDENCIALIDADE

Sumário

1. Política de Segurança da Informação:

1.1. Políticas de segurança da informação:

1.1.1. **ISO/IEC 270017**: Convém ter uma política de segurança da informação específica para a computação em nuvem, que descreva as informações, ativos e processos armazenados nuvem, usuários que utilizam esses serviços e o contexto em que utilizam, os administradores dos serviços em nuvem que têm acesso privilegiado e a localização geográficas de onde os dados dos clientes podem ser armazenados.

1.1.2. ISO/IEC 27018: Convém integrar as práticas de proteção de dados pessoais em computação em nuvem na política de segurança da informação da organização, garantindo que todos os aspectos relevantes sejam abordados. Esses aspectos incluem, avaliação e tratamento de riscos relacionados à proteção de dados pessoais, medidas para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais, aderência às legislações e regulamentos aplicáveis à proteção de dados, definição clara de papéis e responsabilidades dentro da organização, programas de capacitação para colaboradores sobre a importância da proteção de dados, processos para monitorar a eficácia das medidas de segurança e revisar a política regularmente.

1.1.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A SAT SOLUÇÕES EM TECNOLOGIA possui uma política de segurança da informação específica para o ambiente de computação em nuvem, que abrange informações detalhadas sobre os ativos, processos e a localização geográfica de armazenamento dos dados dos clientes. Adicionalmente, a empresa incorpora práticas específicas de proteção de dados pessoais em nuvem, realizando avaliações periódicas de riscos relacionados ao tratamento de dados, implementando medidas de mitigação para assegurar a confidencialidade, integridade e disponibilidade desses dados. Os processos de proteção de dados estão devidamente alinhados com as legislações e regulamentações aplicáveis, e a empresa mantém programas contínuos de capacitação e treinamento para colaboradores, enfatizando a importância da proteção de dados pessoais.

- Neste tópico, não possuem ações a serem realizadas.

2. Organização da segurança da informação:

2.1. Papéis e responsabilidades pela segurança da informação:

2.1.1. **ISO/IEC 27017:** Convém ter documentado um acordo, garantindo que ambas as partes (provedor e cliente) compreendam suas obrigações para com a segurança das informações. Deve-se verificar as responsabilidades na gestão de incidentes de segurança da informação e garantir que essas responsabilidades atendam aos requisitos, incluir programas de conscientização, educação e treinamento sobre segurança da informação para todos os usuários do serviço em nuvem, abordando riscos e procedimentos relevantes, e assegurar que a proteção dos dados e ativos armazenados no serviço em nuvem seja adequada, incluindo a implementação de controles de acesso e a gestão de cópias de segurança.

2.1.2. **ISO/IEC 27018:** A definição de papéis e responsabilidades é fundamental para a implementação eficaz das práticas de proteção de dados pessoais. Para isso deve-se designar indivíduos ou equipes responsáveis pela proteção de dados pessoais e pela implementação das políticas de segurança da informação, definir e comunicar claramente a todos os colaboradores suas responsabilidades garantindo que todos entendam seu papel na proteção de dados, realizar treinamento adequado para desempenhar suas funções de forma eficaz, incluindo a compreensão das obrigações legais e das práticas de segurança, supervisionar e monitorar o cumprimento das responsabilidades atribuídas, assegurando que as práticas de proteção de dados sejam seguidas e revisar os papeis e responsabilidades regularmente para garantir que permaneçam relevantes e eficazes em face de mudanças na organização ou na legislação.

2.1.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A SAT SOLUÇÕES EM TECNOLOGIA já possui responsabilidades claramente definidas para a segurança da informação em computação em nuvem, bem como os indivíduos encarregados de implementar e monitorar as políticas de proteção de dados pessoais nesse ambiente. A SAT SOLUÇÕES EM TECNOLOGIA define e comunica as responsabilidades de todos os colaboradores e realiza treinamentos periódicos sobre o tema, assegurando a conscientização e o alinhamento de toda a equipe com as práticas de segurança e proteção de dados.

- Neste tópico, não possuem ações a serem realizadas.

2.2. Contato com autoridades:

2.2.1. **ISO/IEC 27017:** Convém definir e comunicar para todos os colaboradores quais são as autoridades competentes que podem ser contatadas em relação à segurança da informação em serviços em nuvem caso houver necessidade.

2.2.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre o contato com autoridades além do que já é coberto pela ISO/IEC 27001.

2.2.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA já define claramente as autoridades competentes a serem contatadas em caso de necessidade, incluindo órgãos regulatórios e entidades governamentais de segurança cibernética. Todos os colaboradores estão informados sobre essas autoridades e o procedimento de contato em situações de incidente. A empresa também possui um procedimento documentado com diretrizes sobre quando e como realizar o contato, incorporado na política de segurança da informação.

- Neste tópico, não possuem ações a serem realizadas.

3. Segurança em recursos humanos:

3.1. Conscientização, educação e treinamento em segurança da informação:

3.1.1. **ISO/IEC 27017:** Em treinamentos de conscientização em segurança da informação para serviços em nuvem, devem ser incluídas as instruções sobre os padrões e procedimentos para o uso dos serviços em nuvem, informações sobre os riscos de segurança da informação relacionados ao serviço em nuvem e como esses riscos são gerenciados e as informações sobre a legislação aplicável e considerações regulatórias que impactam o uso de serviços em nuvem.

3.1.2. **ISO/IEC 27018:** Os treinamentos de conscientização sobre proteção de dados pessoais em serviços de nuvem devem ser realizados de forma regular, com atualizações frequentes para refletir mudanças na legislação, nas políticas da organização ou nas ameaças à segurança da informação, bem como manter registros dos treinamentos realizados, incluindo a lista de participantes, o conteúdo abordado e as avaliações, para demonstrar conformidade e para futuras referências.

3.1.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A SAT SOLUÇÕES EM TECNOLOGIA já realiza treinamentos em segurança da informação e, para atender plenamente aos requisitos de conformidade, inclui conteúdos específicos sobre o uso seguro de serviços em nuvem, abordando principais riscos e estratégias de mitigação no contexto de redes e sistemas. Adicionalmente, a empresa promove treinamentos regulares sobre proteção de dados pessoais, destacando obrigações legais, políticas internas e melhores práticas de segurança, com atualizações frequentes para refletir mudanças legais e novas ameaças.

- Neste tópico, não possuem ações a serem realizadas.

4. Gestão de ativos:

4.1. Inventário de ativos:

4.1.1. **ISO/IEC 27017:** Convém que os ativos armazenados em nuvem sejam citados no inventário bem como onde esse ativo é mantido.

4.1.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre o inventário de ativos além do que já é coberto pela ISO/IEC 27001.

4.1.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA, já possui um inventário muito bem estruturado com todos os ativos da empresa, esse inventário é feito na plataforma JIRA onde consta o tipo de ativo, a localização, identificação e status dele.

- Neste tópico, não possuem ações a serem realizadas.

4.2. Rótulos e tratamento de informações:

4.2.1. **ISO/IEC 27017:** As informações e os ativos mantidos em nuvem devem ser rotulados.

4.2.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre a rotulagem e tratamento de informações além do que já é coberto pela ISO/IEC 27001.

4.2.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA aplica rótulos apropriados aos ativos e informações armazenados em nuvem, indicando o nível de confidencialidade exigido para cada ativo.

- Neste tópico, não possuem ações a serem realizadas.

5. Controle de acessos:

5.1. Acessos às redes e aos serviços de rede:

5.1.1. **ISO/IEC 27017:** A política de controle de acesso deve especificar os requisitos para acesso do usuário ao ambiente de nuvem.

5.1.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre os acessos às redes e aos serviços de rede além do que já é coberto pela ISO/IEC 27001.

5.1.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA já possui um controle de acessos bem estruturado e robusto para seus serviços, incluindo um tópico específico na política de controle de acessos que detalha os procedimentos para concessão, gerenciamento e revogação de acessos ao ambiente de nuvem.

- Neste tópico, não possuem ações a serem realizadas.

5.2. Gerenciamento de direito de acesso privilegiado:

5.2.1. **ISO/IEC 27017:** Convém utilizar técnicas adequadas e robustas de controle de acesso para autenticar o usuário privilegiado em serviços de nuvem.

5.2.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre o gerenciamento de direito de acesso privilegiado além do que já é coberto pela ISO/IEC 27001.

5.2.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA já adota técnicas adequadas de autenticação, incluindo a autenticação multifator, para garantir a segurança do acesso administrativo aos serviços em nuvem.

- Neste tópico, não possuem ações a serem realizadas.

5.3. Gerenciamento da informação de autenticação secreta de usuários

5.3.1. **ISO/IEC 27017:** Convém utilizar procedimentos para armazenamento e gerenciamento adequado de senhas.

5.3.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre o Gerenciamento da informação de autenticação secreta de usuários além do que já é coberto pela ISO/IEC 27001.

5.3.3. Ações para estar em conformidade com a ISO/IEC 27017:

o A SAT SOLUÇÕES EM TECNOLOGIA estabelece diretrizes de senhas que exigem a criação de senhas complexas e fortes para os usuários, visando minimizar o risco de ataques de força bruta. O acesso aos sistemas de armazenamento de senhas é restrito exclusivamente a pessoal autorizado, e a empresa implementa monitoramento e auditoria de acesso para detectar tentativas não autorizadas.

o Neste tópico, não possuem ações a serem realizadas.

5.4. Registro de cancelamento do usuário:

5.4.1. **ISO/IEC 27017:** A ISO/IEC 27017 não adiciona novos requisitos específicos sobre o registro e cancelamento do usuário além do que já é coberto pela ISO/IEC 27001.

5.4.2. ISO/IEC 27018: Convém que os procedimentos para registro e cancelamento de usuários devem considerar situações em que o controle de acesso do usuário esteja comprometido. Isso inclui casos como a corrupção ou o comprometimento de senhas ou outros dados de registro do usuário, que podem ocorrer devido a divulgações involuntárias.

5.4.3. Ações para estar em conformidade com a ISO/IEC 27018:

o A SAT SOLUÇÕES EM TECNOLOGIA estabelece procedimentos específicos para o cancelamento imediato de acesso de usuários em casos de comprometimento, como corrupção de senhas ou exposição de dados de autenticação. A empresa também implementa um processo claro de revogação de acesso, que inclui a redefinição de senhas e notificação ao usuário, além de monitoramento contínuo para detectar sinais de comprometimento, como tentativas de login suspeitas. Todas as ações de cancelamento e revogação de acesso são registradas e documentadas, garantindo conformidade e suporte para auditorias futuras.

o Neste tópico, não possuem ações a serem realizadas.

5.5. Procedimentos seguros de entrada no sistema (log-on):

5.5.1. **ISO/IEC 27017:** A ISO/IEC 27017 não adiciona novos requisitos específicos sobre os procedimentos seguros de entrada nos sistemas além do que já é coberto pela ISO/IEC 27001.

5.5.2. **ISO/IEC 27018:** Convém o operador de dados pessoais (DP) em nuvem pública forneça procedimentos seguros de entrada no sistema para quaisquer contas solicitadas pelo cliente que utiliza serviços em nuvem. Isso se aplica a usuários que utilizam serviços em nuvem sob o controle do operador.

5.5.3. Ações para estar em conformidade com a ISO/IEC 27018:

o A SAT SOLUÇÕES EM TECNOLOGIA implementa políticas que exigem senhas fortes e outras medidas de segurança, incluindo limites para tentativas de login e bloqueio automático após múltiplas tentativas malsucedidas. Além disso, configura sessões seguras com tempo de expiração adequado para usuários que acessam os serviços em nuvem, reduzindo o risco de acessos não autorizados em dispositivos deixados sem supervisão.

o Neste tópico, não possuem ações a serem realizadas.

6. Criptografia

6.1. Política para o uso de controle criptográficos:

6.1.1. **ISO/IEC 27017:** Devem ser implementados controles criptográficos para o uso de serviços em nuvem.

6.1.2. ISO/IEC 27018: A norma prescreve que o operador de dados pessoais (DP) em nuvem pública deve fornecer informações ao cliente sobre as circunstâncias em que utiliza a criptografia para proteger os dados pessoais que trata. Além disso, o operador deve informar ao cliente sobre quaisquer capacidades que ele oferece que possam auxiliar o cliente na aplicação de sua própria proteção criptográfica.

6.1.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A SAT SOLUÇÕES EM TECNOLOGIA gerencia a criptografia de dados pelo Google Workspace, garantindo proteção em todas as etapas, tanto no trânsito quanto em segurança, de acordo com as políticas de segurança do Google.

- Neste tópico, não possuem ações a serem realizadas.

6.2. Gerenciamento de chaves:

6.2.1. **ISO/IEC 27017:** Deve-se entender os procedimentos que o provedor de nuvem utiliza, como o tipo de chave, e o procedimento para cada estágio do ciclo de vida das chaves.

6.2.2. ISO/IEC 27018: A ISO/IEC 27018 não adiciona novos requisitos específicos sobre o gerenciamento de chaves além do que já é coberto pela ISO/IEC 27001.

6.2.3. Ações para estar em conformidade com a ISO/IEC 27017:

- Os controles criptográficos da SAT SOLUÇÕES EM TECNOLOGIA garantem que todos os dados sensíveis sejam protegidos por meio de criptografia, de acordo com as políticas de segurança do Google Workspace. Esse controle inclui aplicação automática de criptografia para dados em trânsito e segurança, garantindo que as informações sejam protegidas contra acessos não autorizados.

- Neste tópico, não possuem ações a serem realizadas.

7. Segurança nas operações:

7.1. Gestão de mudanças:

7.1.1. **ISO/IEC 27017:** Convém considerar o impacto que alterações realizadas pelo provedor de nuvem podem causar.

7.1.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre a gestão de mudanças além do que já é coberto pela ISO/IEC 27001.

7.1.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA estabelece um processo para avaliar o impacto de quaisquer alterações realizadas pelo provedor de nuvem na segurança e operação dos dados e serviços da empresa, assegurando que o provedor informe antecipadamente sobre mudanças significativas em infraestrutura, configurações ou políticas de segurança. Isso permite que a empresa realize uma análise de impacto e adote as medidas necessárias. A SAT também possui planos de contingência para responder rapidamente a alterações que possam comprometer a segurança ou a continuidade dos serviços, incluindo ajustes de segurança e backups.

- Neste tópico, não possuem ações a serem realizadas.

7.2. Reutilização e alienação segura de equipamentos:

7.2.1. **ISO/IEC 27017:** Convém que o cliente de serviços em nuvem solicite a confirmação de que o provedor possui políticas e procedimentos para descarte ou ressudo de recursos de forma segura.

7.2.2. ISO/IEC 27018: Para fins de descarte ou reutilização seguros, a norma prescreve que os equipamentos que contêm mídia de armazenamento que possivelmente possa conter dados pessoais (DP) devem ser tratados como se realmente contivessem esses dados. Isso implica que medidas adequadas devem ser tomadas para garantir que os dados não sejam acessíveis após o descarte ou reutilização do equipamento.

7.2.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A SAT SOLUÇÕES EM TECNOLOGIA possui um processo estruturado para o descarte de dados pessoais, garantindo que, ao final do período de retenção, as informações sejam eliminadas de forma segura e irrecuperável.

- Neste tópico, não possuem ações a serem realizadas.

7.3. Separação dos ambientes de desenvolvimento, teste e operação:

7.3.1. ISO/IEC 27017: A ISO/IEC 27017 não adiciona novos requisitos específicos sobre a separação dos ambientes de desenvolvimento, teste e operação além do que já é coberto pela ISO/IEC 27001.

7.3.2. **ISO/IEC 27018**: Quando não for possível evitar a utilização de dados pessoais (DP) para fins de teste, a norma prescreve que uma avaliação de risco deve ser realizada. Isso implica que as organizações devem identificar e avaliar os riscos associados ao uso de DP em ambientes de teste. Além disso, a norma recomenda que medidas técnicas e organizacionais sejam implementadas para minimizar os riscos identificados durante a avaliação.

7.3.3. Ações para estar em conformidade com a ISO/IEC 27018:

o A SAT SOLUÇÕES EM TECNOLOGIA possui uma política de testes seguros, onde são descritos os testes funcionais, de aceitação e de segurança, sempre prezando pela proteção e gestão das informações.

o Neste tópico, não possuem ações a serem realizadas.

7.4. Gestão da capacidade:

7.4.1. **ISO/IEC 27017:** Convém que seja assegurada a capacidade que o provedor de nuvem possui para atender os requisitos, para assegurar o desempenho dos serviços.

7.4.2. ISO/IEC 27018: A ISO/IEC 27018 não adiciona novos requisitos específicos sobre a gestão da capacidade além do que já é coberto pela ISO/IEC 27001.

7.4.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECONOLOGIA já utiliza o Google Workspace, que minimiza riscos e garante a disponibilidade dos serviços. A segurança das informações é mantida de forma contínua, assegurando a confidencialidade, integridade e disponibilidade dos dados.

- Neste tópico, não possuem ações a serem realizadas.

7.5. Cópias de segurança da informação:

7.5.1. ISO/IEC 27017: Convém entender qual a capacidade que o provedor de nuvem possui de armazenamento. Se o provedor de nuvem não ofertar serviços de cópia o próprio cliente deve ser o responsável.

7.5.2. ISO/IEC 27018: A norma prescreve que os sistemas de tratamento de informações baseados em computação em nuvem devem introduzir mecanismos adicionais ou alternativos para cópias de segurança em local remoto. Isso é essencial para proteger contra a perda de dados, assegurar a continuidade das operações de tratamento de dados e permitir a restauração das operações após um evento desastroso**.** É recomendado que múltiplas cópias de dados sejam criadas ou mantidas em locais fisicamente e/ou logicamente diversos, que podem estar dentro do próprio sistema de tratamento de informações, para fins de cópia de segurança e/ou recuperação.

7.5.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- As cópias de segurança dos dados da SAT SOLUÇÕES EM TECNOLOGIA são enviadas para uma empresa contratada, garantindo armazenamento adicional fora da infraestrutura principal. Assim, os dados da organização estão mantidos em segurança reforçando a proteção e a disponibilidade em caso de incidentes locais.

- Neste tópico, não possuem ações a serem realizadas.

7.6. Registro de eventos:

7.6.1. **ISO/IEC 27017:** Convém que sejam definidos quais os requisitos para o registro de log e verificar se o serviço de nuvem fornece esses serviços.

7.6.2. ISO/IEC 27018: A norma prescreve que sempre que possível, os registros de eventos devem indicar se os dados pessoais (DP) foram alterados (adicionados, modificados ou excluídos) como resultado de um evento, e quem realizou essas alterações. O operador de DP em nuvem pública deve estabelecer critérios sobre se, quando e como as informações dos registros podem ser disponibilizadas ou utilizadas pelo cliente que utiliza serviços em nuvem. Esses procedimentos devem ser comunicados ao cliente.

7.6.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A SAT SOLUÇÕES EM TECNOLOGIA mantém registros detalhados e realiza o monitoramento contínuo de suas operações para garantir a segurança e a conformidade. Esses registros incluem registros de acesso, atividades dos usuários e eventos de segurança, permitindo uma visão clara das operações e facilitando a identificação de incidentes ou anomalias.

- Neste tópico, não possuem ações a serem realizadas.

8. Segurança das comunicações:

8.1. Gestão de vulnerabilidades técnicas:

8.1.1. **ISO/IEC 27017:** Convém solicitar informações ao provedor de nuvem sobre como se a gestão de vulnerabilidades que podem afetar os serviços de nuvem fornecidos. Convém verificar quais vulnerabilidades são de responsabilidade do cliente e definir processo para isso.

8.1.2. ISO/IEC 27018: A ISO/IEC 27017 não adiciona novos requisitos específicos sobre a gestão de vulnerabilidades técnicas além do que já é coberto pela ISO/IEC 27001.

8.1.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A gestão de vulnerabilidades técnicas da SAT SOLUÇÕES EM TECNOLOGIA envolve a identificação, avaliação e mitigação de pontos fracos potenciais nos sistemas. Esse processo inclui a realização de varreduras periódicas para detectar vulnerabilidades, aplicação de patches de segurança e atualização constante de sistemas e softwares.

- Neste tópico, não possuem ações a serem realizadas.

8.2. Segregação de redes:

8.2.1. **ISO/IEC 27017:** Convém que o cliente do serviço em nuvem defina os requisitos para a segregação de redes, para obter o devido isolamento do ambiente compartilhado e verificar se o provedor de nuvem atende a esses requisitos.

8.2.2. ISO/IEC 27018: A ISO/IEC 27018 não adiciona novos requisitos específicos sobre a segregação de redes além do que já é coberto pela ISO/IEC 27001.

8.2.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA possui a segregação de rede estabelecida em três principais categorias: gerência, usuários e visitantes. Essa segmentação contribui significativamente para a segurança, limitando o acesso entre as diferentes áreas da rede.

- Neste tópico, não possuem ações a serem realizadas.

8.3. Políticas e procedimentos para a transferência de informações:

8.3.1. **ISO/IEC 27017:** A ISO/IEC 27017 não adiciona novos requisitos específicos sobre as Políticas e procedimentos para a transferência de informações redes além do que já é coberto pela ISO/IEC 27001.

8.3.2. **ISO/IEC 27018:** Quando mídias físicas são utilizadas para a transferência de informações que contêm dados pessoais (DP), é recomendado que um sistema seja implementado para registrar a entrada e a saída dessas mídias. Esse registro deve incluir informações como o tipo de mídia, os remetentes e destinatários autorizados, a data e hora, e a quantidade de mídia. Sempre que possível, os clientes que utilizam serviços em nuvem devem ser incentivados a implementar medidas adicionais, como a criptografia, para garantir que os dados possam ser acessados apenas no ponto de destino e não durante o transporte.

8.3.3. Ações para estar em conformidade com a ISO/IEC 27018:

- A SAT SOLUÇÕES EM TECNOLOGIA realiza a transferência de informações de forma segura, utilizando ferramentas em nuvem e protocolos confiáveis para garantir a proteção dos dados durante o envio e a coleta. A criptografia é aplicada tanto em trânsito quanto em repouso, garantindo que as informações sejam mantidas seguras e íntegras durante toda a transferência.

- Neste tópico, não possuem ações a serem realizadas.

9. Aquisição, desenvolvimento e manutenção de sistemas:

9.1. Análise e especificação dos requisitos de segurança da informação:

9.1.1. **ISO/IEC 27017:** Convém que o cliente dos serviços de nuvem defina os requisitos e avalie se o provedor os realiza de forma adequada. Convém verificar quais são as práticas e procedimentos de desenvolvimento seguro utilizada pelo provedor de nuvem.

9.1.2. ISO/IEC 27018: A ISO/IEC 27018 não adiciona novos requisitos específicos sobre as Aquisição, desenvolvimento e manutenção de sistemas além do que já é coberto pela ISO/IEC 27001.

9.1.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A aquisição, o desenvolvimento e a manutenção de sistemas na SAT SOLUÇÕES EM TECNOLOGIA seguem critérios rigorosos de segurança para garantir a proteção dos dados e a conformidade com as políticas internacionais.

- Neste tópico, não possuem ações a serem realizadas.

10. Relacionamento na cadeia de suprimento:

10.1. Política de segurança da informação no relacionamento om os fornecedores:

10.1.1. **ISO/IEC 27017:** Incluir o provedor de nuvem na política de fornecedores, isso ajudará a mitigar os riscos causados pelo provedor de nuvem, como riscos de acessos e gestão.

10.1.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre as Política de segurança da informação no relacionamento om os fornecedores além do que já é coberto pela ISO/IEC 27001.

10.1.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A política de segurança da informação na cadeia de fornecimento é tratada com rigor pela SAT SOLUÇÕES EM TECNOLOGIA, garantindo que todos os fornecedores e parceiros estejam alinhados aos padrões de segurança exigidos

- Neste tópico, não possuem ações a serem realizadas.

10.2. Identificando a segurança da informação nos acordos com os fornecedores:

10.2.1. **ISO/IEC 27017:** Convém verificar as responsabilidades que o provedor de nuvem possui para com o cliente, como por exemplo proteção contra malware, cópias de segurança, controles criptográficos, gestão de vulnerabilidades, gestão de incidentes, verificação de conformidade técnica, testes de segurança, auditoria, coleta, armazenamento e proteção de logs, proteção das informações após finalização do contrato, autenticação e controle de acesso, gestão de identidades e acessos.

10.2.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novas informação específicas sobre o requisito identificando a segurança da informação nos acordos com os fornecedores além do que já é coberto pela ISO/IEC 27001.

10.2.3. Ações para estar em conformidade com a ISO/IEC 27017:

- O gerenciamento da entrega de serviços dos fornecedores na SAT SOLUÇÕES EM TECNOLOGIA inclui práticas para garantir que eles cumpram os requisitos de segurança e qualidade estabelecidos. A organização monitora o desempenho dos fornecedores, verificando se os serviços são entregues em conformidade com as especificações acordadas e os padrões de segurança

- Neste tópico, não possuem ações a serem realizadas.

11. Gerenciamento de incidentes de segurança da informação:

11.1. Responsabilidades e procedimentos:

11.1.1. **ISO/IEC 27017:** Convém que o cliente de serviço em nuvem verifique a atribuição de responsabilidades da gestão de incidentes de segurança da informação e garanta que os requisitos sejam atendidos.

11.1.2. ISO/IEC 27018: A norma prescreve que, quando um incidente de segurança da informação ocorre, deve ser realizada uma análise crítica pelo operador de dados pessoais (DP) em nuvem pública. Essa análise é parte do processo de gestão de incidentes e visa determinar se houve uma violação de dados que envolva DP. É importante distinguir entre um incidente e um evento de segurança da informação. Um evento não necessariamente resulta em uma análise crítica, especialmente se não houver uma probabilidade real ou significativa de acesso não autorizado aos DP ou aos equipamentos que armazenam esses dados. Exemplos de eventos incluem pings, varreduras de portas e tentativas malsucedidas de log-on.

11.1.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A gestão de incidentes de segurança da informação na SAT SOLUÇÕES EM TECNOLOGIA envolve processos bem definidos para identificar, responder e resolver incidentes de forma rápida e eficaz.

- Neste tópico, não possuem ações a serem realizadas.

11.2. Notificação de eventos de segurança da informação:

11.2.1. **ISO/IEC 27017:** Convém que o cliente em nuvem notifique os provedores os eventos que foram detectados e acompanhe o estado desses eventos.

11.2.2. ISO/IEC 27018: A ISO/IEC 27018 não adiciona novos requisitos específicos sobre a notificação de eventos de segurança da informação além do que já é coberto pela ISO/IEC 27001.

11.2.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- O relacionamento na cadeia de fornecimento da SAT SOLUÇÕES EM TECNOLOGIA é gerenciado com foco na segurança e na conformidade, garantindo que todos os fornecedores e parceiros atendam aos requisitos de proteção de dados e segurança da informação.

- Neste tópico, não possuem ações a serem realizadas.

12. Conformidade:

12.1. Identificação da legislação aplicável e de requisitos contratuais:

12.1.1. **ISO/IEC 27017:** Convém que o cliente em nuvem requisite a evidência de conformidade do provedor com as normas e regulamentações relevantes e requeridas pelo negócio.

12.1.2. **ISO/IEC 27018:** A ISO/IEC 27018 não adiciona novos requisitos específicos sobre a Identificação da legislação aplicável e de requisitos contratuais além do que já é coberto pela ISO/IEC 27001.

12.1.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA realiza revisões regulares para garantir que todos os processos e controles sejam atualizados e estejam em conformidade com os critérios legais, bem como com os termos contratuais estabelecidos com clientes e parceiros.

- Neste tópico, não possuem ações a serem realizadas.

12.2. Direito de propriedade intelectual:

12.2.1. **ISO/IEC 27017:** Convém que o cliente em nuvem esteja ciente que a instalação de software licenciado em um serviço em nuvem pode violar os termos de licença. Portanto é recomendável que o cliente tenha procedimentos para identificar os requisitos de licenciamento específicos para ambientes em nuvem antes de instalar qualquer software.

12.2.2. ISO/IEC 27018: A ISO/IEC 27018 não adiciona novos requisitos específicos sobre o direito de propriedade intelectual que já é coberto pela ISO/IEC 27001.

12.2.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA adota uma política que impede os usuários de instalar software nas máquinas, garantindo que apenas programas autorizados e monitorados sejam executados.

- Neste tópico, não possuem ações a serem realizadas.

12.3.Proteção de registros:

12.3.1. **ISO/IEC 27017:** Convém que o cliente em nuvem requisite ao provedor de nuvem a informação sobre a proteção dos registros controlados e armazenados no provedor.

12.3.2. ISO/IEC 27018: A ISO/IEC 27018 não adiciona novos requisitos específicos sobre a proteção de registros que já é coberto pela ISO/IEC 27001.

12.3.3. Ações para estar em conformidade com a ISO/IEC 27017:

- A SAT SOLUÇÕES EM TECNOLOGIA possui medidas de segurança aplicadas para assegurar a confidencialidade, integridade e disponibilidade dos registros. Os acordos ou contratos firmados com o provedor de nuvem descrevem requisitos específicos para a proteção desses registros, detalhando as práticas de segurança que o provedor deve manter para garantir a proteção dos dados da empresa.

- Neste tópico, não possuem ações a serem realizadas.

12.4. Análise crítica independente de segurança da informação:

12.4.1. **ISO/IEC 27017:** Convém que o cliente em nuvem requisite evidência documentada de que a implementação das diretrizes e controles de segurança do serviço em nuvem estão alinhadas com as informações feitas pelo provedor, tal evidência pode incluir certificações nas normas pertinentes.

12.4.2. ISO/IEC 27018: A norma prescreve que, nos casos em que auditorias individuais do cliente que utiliza serviços em nuvem forem impraticáveis ou puderem aumentar os riscos de segurança, o operador de dados pessoais (DP) em nuvem pública deve disponibilizar aos clientes potenciais evidências independentes de que a segurança da informação está sendo implementada e operada de acordo com as políticas e procedimentos do operador.

12.4.3. Ações para estar em conformidade com a ISO/IEC 27017 e 27018:

- A análise crítica da segurança da informação na SAT SOLUÇÕES EM TECNOLOGIA é realizada regularmente pela alta direção para garantir que as políticas, controles e práticas de segurança estejam alinhados aos objetivos de proteção de dados e segurança.

- Neste tópico, não possuem ações a serem realizadas.

13. Atendimento dos controles:

CONTROLES	NÍVEL DE ATENDIMENTO
Política de segurança da informação	**Conforme**
Papéis e responsabilidades pela segurança da informação	**Conforme**
Contato com autoridades	**Conforme**
Conscientização, educação e treinamento em segurança da informação	**Conforme**
Inventário de ativos	**Conforme**
Rótulos e tratamento de informações	**Conforme**
Acessos às redes e aos serviços de rede	**Conforme**
Gerenciamento de direito de acesso privilegiado	**Conforme**
Gerenciamento da informação de autenticação secreta de usuários	**Conforme**
Registro de cancelamento do usuário:	**Conforme**
Procedimentos seguros de entrada no sistema (log-on):	**Conforme**
Política para o uso de controle criptográficos	**Conforme**
Gerenciamento de chaves	**Conforme**
Gestão de mudanças	**Conforme**
Reutilização e alienação segura de equipamentos	**Conforme**
Separação dos ambientes de desenvolvimento, teste e operação	**Conforme**
Gestão da capacidade	**Conforme**

Cópias de segurança da informação	**Conforme**
Registro de eventos	**Conforme**
Gestão de vulnerabilidades técnicas	**Conforme**
Segregação de redes	**Conforme**
Políticas e procedimentos para a transferência de informações	**Conforme**
Análise e especificação dos requisitos de segurança da informação	**Conforme**
Política de segurança da informação no relacionamento om os fornecedores	**Conforme**
Identificando a segurança da informação nos acordos com os fornecedores	**Conforme**
Responsabilidades e procedimentos	**Conforme**
Notificação de eventos de segurança da informação	**Conforme**
Identificação da legislação aplicável e de requisitos contratuais	**Conforme**
Direito de propriedade intelectual	**Conforme**
Proteção de registros	**Conforme**
Análise crítica independente de segurança da informação	**Conforme**

4. RESULTADO FINAL

A SAT SOLUÇÕES EM TECNOLOGIA apresenta alta maturidade nos processos de segurança da informação e está em plena conformidade com os principais requisitos das normas ISO/IEC 27017 e ISO/IEC 27018. A empresa já possui todos os processos e controles necessários implementados, atendendo integralmente aos requisitos de segurança para o ambiente de computação em nuvem e proteção de dados pessoais.

Recomendações Finais:

1. **Treinamentos Contínuos**: Manter um programa regular de capacitação obrigatória para os colaboradores, abordando práticas de segurança da informação e proteção de dados pessoais, assegurando a conscientização constante sobre as melhores práticas e atualizações normativas.

2. **Monitoramento e Auditoria**: Realizar monitoramento contínuo e auditorias periódicas dos processos de segurança e conformidade, garantindo a eficácia das medidas implementadas e identificando, de forma proativa, áreas que possam requerer ajustes.

3. **Manutenção da Documentação de Conformidade**: Revisar e atualizar a documentação dos processos e controles periodicamente, mantendo evidências claras para auditorias futuras e assegurando alinhamento contínuo com as exigências das normas ISO/IEC 27017 e ISO/IEC 27018.

5. CONCLUSÃO

A SAT SOLUÇÕES EM TECNOLOGIA está em conformidade com as normas ISO/IEC 27017 e ISO/IEC 27018, com os processos e controles necessários implementados para o ambiente de computação em nuvem. A continuidade dos treinamentos obrigatórios e o monitoramento constante dos processos garantirão que a organização mantenha sua robustez em segurança e proteção de dados, permanecendo alinhada com os padrões internacionais de conformidade em nuvem.

6. CONTATO E APROVAÇÕES

Este relatório foi elaborado pela equipe de diagnóstico e aprovado pela direção técnica da blwinner.

Contato Operacional: Gabriella Vianna de Barros Siqueira - Consultora

Telefone: (19) 991410330

E-mail: gabriella.siqueira@blwinner.com.br

Contato Comercial: Lucas Basques da Silva – Gestor Comercial

Telefone: (11) 98983-6965

E-mail: lucasbasques@blwinner.com.br

Contato Operacional: Bene Luiz – Diretor Técnico

Telefone: (13) 99111-6983

E-mail: beneluiz@blwinner.com.br