Controles de Segurança do Processador LGPD

Conteúdo

1 Introdução

A Cobmais é um provedor de serviços bem-sucedido com usuários em muitos países e leva muito a sério a proteção dos dados de seus clientes. A fim de fornecer um nível maior de proteção, a Cobmais investiu em um alto nível de segurança da informação e também adotou controles e melhores práticas definidos nos códigos de prática de segurança da informação.

Um componente-chave desses controles é a definição clara da divisão de responsabilidades entre o provedor de serviços e o cliente. Também é importante que os controles técnicos, processuais e físicos implementados pela Cobmais como parte de seus serviços sejam compreendidos pelo cliente para que uma avaliação dos riscos aos seus dados pessoais possa ser feita.

O objetivo deste documento é descrever em linhas gerais os controles que estão em vigor, ou são oferecidos como opção, dentro do nosso ambiente de tratamento.

A computação em nuvem é geralmente consiste nos seguintes tipos de serviços:

Software como serviço (SaaS) - o fornecimento de um aplicativo hospedado para uso como parte de um processo de negócios. A hospedagem geralmente inclui todos os componentes de suporte para o aplicativo, como hardware, software operacional, bancos de dados etc.

2 Controles de Segurança do Operador na LGPD

As informações a seguir são fornecidas para ajudar nossos clientes a fazer uma escolha informada sobre o nível de segurança das informações que eles acreditam necessários para proteger os dados pessoais, com base em uma avaliação de risco para seus negócios.

As informações fornecidas pretendem refletir um nível de detalhes apropriado sobre nossas defesas de segurança, sem divulgar detalhes que possam ser valiosos para um invasor. Mais detalhes podem estar disponíveis para clientes autorizados sob um acordo de não divulgação, mediante solicitação.

2.1 Política de segurança da informação

As políticas de segurança de informações da Cobmais são previstas considerando as necessidades específicas de fornecimento de serviços em nuvem, incluindo:

- Uso extensivo da virtualização
- A natureza *multi-tenanted* dos nossos serviços
- Riscos de iniciados autorizados
- Proteção de dados do cliente na nuvem
- A necessidade de comunicação efetiva com nossos clientes

Todas as políticas são controladas por versão, autorizadas e comunicadas a todos os funcionários e contratados relevantes.

2.2 Organização da segurança da informação

As funções e responsabilidades para o gerenciamento do ambiente de nuvem são claramente definidas como parte da negociação do contrato, de modo que as expectativas do cliente estejam alinhadas adequadamente com a maneira como o serviço será entregue.

Além disso, uma divisão clara de responsabilidades entre a Cobmais e nossos fornecedores, incluindo provedores de serviços de nuvem que fornecem serviços de suporte, é estabelecida e mantida.

A Cobmais opera a partir de várias regiões geográficas e adota uma abordagem de zona para o armazenamento de dados do cliente.

2.3 Segurança dos recursos humanos

Um programa abrangente de treinamento de conscientização é entregue de forma contínua a todos os funcionários da Cobmais para enfatizar a necessidade de proteger adequadamente os dados da nuvem do cliente. Também exigimos que nossos contratados forneçam treinamento de conscientização adequado a todos os funcionários relevantes.

2.4 Gestão de ativos

A funcionalidade é fornecida sempre que possível dentro dos nossos serviços em nuvem para permitir que nossos clientes reflitam seus próprios esquemas de classificação e rotulagem de informação.

Um procedimento auditado está em vigor para a devolução e remoção de ativos do cliente da nuvem quando apropriado. Este procedimento é projetado para assegurar a proteção dos dados do cliente em geral e particularmente dados pessoais.

2.5 Controle de acesso

Fornecemos uma interface de administração abrangente e amigável ao usuário para administradores de clientes autorizados que permite controlar o acesso no nível de serviço, função e dados. O registro do usuário e o cancelamento de registro e o gerenciamento de direitos de acesso são obtidos por meio dessa interface, cujo acesso futuramente será protegido, se necessário, pela autenticação multifatores.

Procedimentos documentados para a alocação e gerenciamento de informações secretas de autenticação, como senhas, garantem que essa atividade seja conduzida de maneira segura.

O uso de programas utilitários dentro do ambiente de nuvem do cliente por funcionários da Cobmais é estritamente controlado e auditado regularmente.

Nos locais em que operamos um ambiente com múltiplas concessões, os recursos do cliente na nuvem estão sujeitos a segregação lógica, de modo que nenhum acesso é permitido a nenhum aspecto do ambiente de outro cliente, incluindo configurações e dados.

O fortalecimento da máquina virtual, incluindo o fechamento de portas e protocolos desnecessários, é implementado como prática padrão e cada máquina virtual é configurada com o mesmo grau de proteção para malware que os servidores físicos.

2.6 Criptografia

As transações entre o usuário (incluindo administradores) e o ambiente de nuvem são criptografadas usando TLS por padrão. Os dados do cliente são criptografados em repouso usando chaves gerenciadas pela Cobmais.

2.7 Segurança física e ambiental

A Cobmais tem procedimentos em vigor para o descarte seguro e a reutilização de recursos quando não são mais exigidos pelo cliente da nuvem. Esses procedimentos garantirão que os dados do cliente não sejam colocados em risco.

2.8 Segurança de operações

A Cobmais informa os clientes sobre alterações planejadas que afetarão o ambiente ou os serviços de nuvem do cliente. Essas informações são publicadas regularmente em nosso site e via e-mail para os administradores do cliente afetados e incluirão o tipo de alteração, a data e a hora agendadas e, quando apropriado, os detalhes técnicos da alteração feita. Notificações adicionais serão emitidas no início e no final da alteração.

A capacidade do ambiente de nuvem geral está sujeita a monitoramento regular pelos engenheiros da Cobmais para garantir que nossas obrigações de capacidade possam ser cumpridas em todos os momentos.

Os backups criptografados dos ambientes do cliente são levados para uma frequência especificada pela Cobmais e são retidos por um período padrão de três meses. Os backups são armazenados em um único datacenter, com planejamento para armazenar em locais separado com a localização principal dos dados do cliente a uma distância considerada suficiente para representar uma precaução razoável de continuidade de negócios. As amostras de backup são verificadas regularmente para confirmar sua integridade. Restauração de backup pode ser solicitada pelo cliente no dia seguinte.

Registros de atividades e transações são registrados no ambiente de nuvem e podem ser acessados pelos administradores do cliente. Estes incluem detalhes de logins/logouts, acesso a dados e alterações / exclusões.

Todos os relógios do sistema e do dispositivo no ambiente de nuvem são sincronizados (por meio de servidores designados) para uma fonte de horário externa, cujos detalhes estão disponíveis mediante solicitação.

O ambiente de nuvem do cliente está sujeito à verificação regular de vulnerabilidades usando ferramentas padrão do setor. Patches de segurança críticos são aplicados de acordo com as recomendações dos fabricantes de software.

As atividades operacionais que são consideradas críticas e, em alguns casos, irreversíveis (como a exclusão de servidores virtuais) estão sujeitas a procedimentos especialmente controlados que garantem que a verificação adequada seja realizada antes da conclusão. Também recomendamos que o cliente coloque seus próprios procedimentos em prática nessas áreas.

Os recursos de monitoramento de serviço documentados podem ser contratados de forma terceirizada pelo próprio cliente, permitindo que eles monitorem seu ambiente por abusos, como vazamento de dados e controle não autorizado de servidores, etc., em conjunto com o acesso a informações de registro

2.9 Segurança das comunicações

Quando um ambiente de múltiplas locações é fornecido, as redes de clientes da nuvem são isoladas umas das outras. A rede interna da Cobmais também opera de forma isolada de todas as redes e ambientes de clientes.

A configuração dos recursos da rede virtual está sujeita ao mesmo nível de controle dos dispositivos de rede física, de acordo com nossa política de segurança de rede documentada.

2.10 Aquisição, desenvolvimento e manutenção de sistema

Práticas e procedimentos de desenvolvimento seguros são usados naCobmais, incluindo a separação de ambientes de desenvolvimento, teste e produção, técnicas seguras de codificação e testes abrangentes de aceitação de segurança.

2.11 Relações com fornecedores

Na entrega de certos serviços, a Cobmais faz uso de provedores de serviços de nuvem de mesmo nível em um acordo de cadeia de fornecimento. Esses fornecedores estão sujeitos a uma auditoria regular de segunda parte para garantir que eles tenham objetivos definidos para segurança da informação e realizem práticas eficazes de avaliação e tratamento de riscos.

Todos os relacionamentos com fornecedores são cobertos por termos contratuais que atendem aos requisitos da LGPD.

2.12 Gerenciamento de incidentes de segurança da informação

Onde a Cobmais pode julgar apropriado informar o cliente sobre um evento de segurança da informação (antes de determinar se ele deve ser tratado

como um incidente) faremos isso ao administrador ou representante do cliente nomeado. Da mesma forma, o cliente pode relatar eventos de segurança para nossa central de suporte, onde eles serão registrados e a ação apropriada será decidida. Informações sobre o progresso de tais eventos podem ser obtidas no suporte técnico.

A Cobmais relata incidentes de segurança da informação ao cliente, onde acredita que o serviço ou os dados do cliente foram ou serão afetados. Faremos isso com o administrador ou o representante do cliente indicado assim que possível e compartilharemos o máximo de informações sobre o impacto e a investigação do incidente, conforme julgarmos apropriado para sua resolução efetiva e oportuna. Um gerente de incidentes será nomeado em cada caso, que atuará como o ponto de contato da Cobmais para o incidente, incluindo assuntos relacionados à captura e preservação de evidências digitais, se necessário.

Priorizamos as atividades de gerenciamento de incidentes para garantir que os requisitos de tempo da LGPD para notificação de violações que afetam os dados pessoais sejam atendidos.

2.13 Aspectos de segurança da informação do gerenciamento de continuidade de negócios

A Cobmais planeja e testa regularmente, sua resposta a vários tipos de incidentes disruptivos que podem afetar o atendimento ao cliente na nuvem. A arquitetura de nossos serviços de nuvem é projetada para minimizar a probabilidade e o impacto de tal incidente e faremos todos os esforços razoáveis para evitar qualquer impacto nos serviços de nuvem do cliente.

2.14 Conformidade

Os registros coletados pela Cobmais como parte de seu fornecimento do serviço em nuvem estarão sujeitos a proteção de acordo com nosso esquema de classificação de informações e procedimentos de gerenciamento de ativos.