cegid

Medidas Técnicas e Organizativas

junho 2025

Medidas Técnicas e Organizativas

O presente documento faz parte integrante do Contrato (nos termos definidos na cláusula 1.1. (e) das Condições Gerais de Licenciamento).
O Cliente declara e reconhece que as medidas técnicas e organizativas descritas nos Termos do Tratamento e Medidas Técnicas e Organizativas são adequadas ao tratamento de dados levado a cabo pela em seu nome.

Segurança do Tratamento

A Cegid implementa as medidas técnicas e organizativas adequadas para assegurar um nível de segurança dos dados pessoais tratados para as suas próprias finalidades e em nome e por conta do Cliente. Essas medidas técnicas e organizativas a adotar nas atividades de tratamento levadas a cabo pela Cegid em nome e por conta do Cliente são definidas de acordo com a informação introduzida pelo Cliente nos Termos do Tratamento e a regular utilização do software e das suas funcionalidades nos termos do Contrato.
Tendo em conta o Software e Serviço prestado aos seus clientes, a Cegid definiu um conjunto de MEDIDAS CONCRETAS que serão adotadas para cada nível de serviço:

SEGURANÇA	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
Política de palavra-passe forte Existe uma política de palavra-passe forte definida para Utilizadores e administradores das aplicações	●	●	●	●	●	●	●
Autenticação Multi fator A autenticação de todos os utilizadores pode ser feita através de dois ou mais fatores, por exemplo palavra passe e confirmação no smartphone	●	●	●	●	○	○	○
Credenciais auto expiradas As credenciais dos utilizadores expiram no tempo	●	○	○	○	●	○	○
Notificação por inatividade e data do último acesso Identifica utilizadores que não acedem há mais de X dias e informa a data do último acesso	○[1]	●	●	●	○	○	○
Data, hora e endereço IP do ultimo acesso Existem logs com informações sobre o último acesso dos utilizadores às aplicações/serviços	○[1]	●	●	●	●	●	●

SEGURANÇA	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
Auditorias externas regulares Existem auditorias, testes de penetração e vulnerabilidades executados por entidades externas à infraestrutura onde estão instaladas as aplicações	●	●	●	●	●	●	●
SOC – Centro de Operações de Segurança Os sistemas em causa são monitorizados por equipas de segurança que trabalham 24x7	▨[1]	▨[1]	▨[1]	▨[1]	●	▨[1]	●
Antivírus Os sistemas têm antivírus instalados e atualizados	●	●	●	●	●	●	●
Utilização de TLS versão mais recente As comunicações entre os diferentes sistemas utilizam os mais modernos protocolos de encriptação da informação	●	●	●	●	●	●	●
Palavras-passe cifradas Todas as credenciais guardadas em código, ficheiros de configuração ou em bases de dados estão encriptadas por HASH-256 mínimo	●	●	●	●	●	○	●
Segurança dos dados armazenados Os sistemas utilizam pelo menos um tipo de encriptação da informação: FileSystem, Database ou Full Disk	●	●	●	●	●	●	●
Informação pessoal cifrada/anonimizada na BD Todos os dados pessoais contidos em BD ou em ficheiros estão cifrados ou anonimizados	●	●	●	●	○	○	○
URL sem variáveis visíveis Todos os URLs estão isentos de variáveis de sessão e sem dados pessoais	●	●	●	●	●	●	●
Não é guardada informação pessoal além do tempo da sessão Não é guardada informação pessoal no navegador, disco ou memória, por exemplo no formato de cookies, para além do tempo da sessão e apenas na medida do necessário	●	●	●	●	●	●	●
Transmissão segura de credenciais Todas as credenciais são transmitidas em HASH mínimo SHA-256	●	●	●	●	●	●	●
Comunicações criptografadas Sessão segura com protocolo de segurança SSL/TLS ou HTTPS	●	●	●	●	●	●	●
Comunicação segura entre camadas Comunicação com camadas FE ou BD através de sessão segura	●	●	●	●	●	●	●
Utilização de boas práticas de DNSSec, SPF, DKIM, IP fixo, … Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados	●	●	●	●	●	●	●
DoS protection Proteção contra ataques do tipo negação de serviço	●	●	●	●	●	●	●

SEGURANÇA	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
Proteção perimétrica Ferramentas de deteção de ameaças na defesa perimétrica	●	●	●	●	●	●	●
Deteção de atividades maliciosas Utilização de IDS para monitorizar e detectar atividades maliciosas ou violações das políticas de segurança	●	●	●	●	●	●	●
Registos "CRUD" São guardados registos (logs) com informação sobre as ações efetuadas sobre os dados (create, read, update, delete)	▨[2]	▨[2]	▨[2]	▨[2]	▨[2]	▨[2]	▨[2]
Testes de Engenharia social Existe formação regular em segurança e são executadas atividades de engenharia social com todos os colaboradores da PRIMAVERA	●	●	●	●	●	●	●
Integridade dos registos (logs) Todos os registos (logs) são armazenados apenas em modo de leitura com garantia de integridade	●	●	●	●	●	●	●
Registos de acesso São guardados registos de atividades de acesso e de tentativas falhadas	●	●	●	●	●	●	●
Fim do tempo de sessão Políticas de fim de sessão para terminais e aplicações remotas	●	●	●	●	●	●	●

BACKUP & RECOVERY	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
Política de cópias de segurança São realizadas cópias de segurança diárias para todos os Dados armazenados	●	●	●	●	●	●	●
Armazenamento seguro das cópias de segurança Cifragem e assinatura digital para as cópias de segurança	●	●	●	●	●	●	●
Cópia de segurança para local remoto Cópias de segurança efetuadas para locais físicos distintos, com periodicidade mínima semanal	●	●	●	●	●	●	●
Testes às cópias de segurança Existem e são executados testes regulares às cópias de segurança e aos procedimentos de reposição dessas cópias	●	●	●	●	●	●	●

FRAMEWORKS	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
ITIL	○	●	●	●	●	●	●
SCRUM	●	●	●	●	●	●	●
ISO9001	●	●	●	●	●	●	●
CMMI	○	●	●	●	●	●	●

DATACENTER	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
ISO 20000	○	●	●	●	●	●	●
ISO 22301	○	●	●	●	●	●	●
ISO 27001	●	●	●	●	●	●	●
ISO 27017	○	●	●	●	●	●	●
ISO 27017	○	●	●	●	●	●	●
ISO 27018	○	●	●	●	●	●	●
ISO 9001	●	●	●	●	●	●	●
SOC 1, SOC 2 & SOC 3	○	●	●	●	●	●	●

DATACENTER	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
GDPR	○	●	●	●	●	●	●
EU-US Privacy Shield	○	●	●	●	●	●	●
EU Model Clauses	○	●	●	●	●	●	●
EN 301 549 (EU)	○	●	●	●	●	●	●
ENISA IAF (EU)	○	●	●	●	●	●	●

SLAs	XRP Enterprise	ROSE	Jasmin	Invoicing Engine	SaaS Partilhado	Omnia v2	Omnia v3
Disponibilidade >= 99,5% mês	●	●	●	●		●	●
Tempo de resposta a tickets de suporte	**Desde 12h para tickets com prioridade Crítical até 24h para tickets com prioridade Planning** (horas úteis, horário de Portugal Continental)	**Desde 12h para tickets com prioridade Crítical até 24h para tickets com prioridade Planning** (horas úteis, horário de Portugal Continental)	**Desde 6h para tickets com prioridade Crítical até 18h para tickets com prioridade Planning** (horas úteis, horário de Portugal Continental)	**Desde 12h para tickets com prioridade Crítical até 24h para tickets com prioridade Planning** (horas úteis, horário de Portugal Continental)	**Desde 12h para tickets com prioridade Crítical até 24h para tickets com prioridade Planning** (horas úteis, horário de Portugal Continental)	**Desde 6h para tickets com prioridade Crítical até 18h para tickets com prioridade Planning** (horas úteis, horário de Portugal Continental)	**Desde 6h para tickets com prioridade Crítical até 18h para tickets com prioridade Planning** (horas úteis, horário de Portugal Continental)

● **Sim**

○ **Não**

[1] **O Serviço é suportado em PaaS pelo que a monitorização é realizada diretamente pela Microsoft**

[1] ○ **Não notifica, mas pode ver a informação**

[2] **Nem todas as operações ou tabelas têm logs e em alguns casos a ativação desses logs é da responsabilidade do cliente/Parceiro**

[1] * **A cópia de segurança remota pode ser assegurada pelo Parceiro com a periodicidade que quiser**

cegid