Política de Segurança

versão 1.1

07 de agosto de 2025

Política de Segurança

1. Objetivo

A Política de Segurança da Lepidus é uma declaração formal acerca do nosso comprometimento com a proteção dos ativos de informações de nossa propriedade ou sob nossa guarda, devendo ser cumprida e respeitada por todos os integrantes da empresa. Tem como objetivo a implantação de políticas de segurança visando garantir a integridade, disponibilidade e autenticidade dos dados, descritas por tópicos neste documento.

2. Política de cópia de segurança (backup)

A política de backup objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Lepidus e formalmente definidos como necessários, para se manter a continuidade do negócio. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. A seguir são apresentadas as políticas de backup, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados.

A periodicidade, tempo de armazenamento e quantidade de cópias podem ser ajustados por contrato / termo aditivo. Exemplos de personalizações comuns são: ampliar o tempo mínimo para armazenamento do backup e ter uma cópia armazenada em servidor de responsabilidade do cliente.

Apenas membros da equipe de segurança e infraestrutura da Lepidus têm acesso aos backups, reduzindo-se o número de pessoas que possam ter acesso a informações confidenciais.

Os procedimentos de backup são executados de forma automatizada, pelo menos uma vez ao dia, ou mais vezes quando indicado em contrato/procedimento específico. Deve-se priorizar a criação de backups em horários de baixo tráfego e de forma a ter o menor impacto possível na experiência de uso da aplicação.

Os backups serão mantidos por, no mínimo, uma semana e armazenados em pelo menos **dois** locais geograficamente distantes (em cidades diferentes). Uma das cópias precisa ser armazenada necessariamente em um fornecedor distinto ao que fica hospedada a aplicação.

> Exemplo: A aplicação OJS está hospedada no serviço VPS da Akamai (Linode), enquanto o seu backup é armazenado no serviço S3 da Amazon Web Services (AWS) e uma segunda cópia fica armazenada no S3 do provedor Vultr.

Após o período indicado, as cópias de segurança serão inutilizadas, de modo que, após este prazo, devem ser consideradas sem possibilidade de recuperação.

São feitos testes, mensalmente ou mais frequentemente, para validar os múltiplos backups estão funcionais, assegurando que é possível restaurar a aplicação na íntegra a partir dos dados de qualquer período de retenção e de, no mínimo, dois armazenamentos distintos. Após os testes, deve ser feito um relatório visando atestar, validar e indicar possíveis aperfeiçoamentos nos procedimentos de backups em diversos cenários, como: restauração da aplicação com maior volume de dados, restauração de um conjunto maior de dados simultaneamente, se o software de backup está adequado, sendo ativamente mantido e se a política de backup atende às melhores práticas.

A escolha de onde e como são armazenados os backups tem como objetivo, além da preservação dos dados, reduzir o tempo de restabelecimento do serviço em caso de desastre.

3. Política de Proteção de Dados Pessoais e Privacidade

Vide documento de Política Institucional de Proteção de Dados Pessoais.

4. Tempos de atendimento em caso de incidentes

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança, levando a perda de um dos princípios da Segurança da Informação, mencionados anteriormente.
São exemplos de incidentes de segurança:

- Tentativas de ganhar acesso não autorizado a sistemas ou dados lógicos, ou físicos;
- Indisponibilidade de informações e dados para a execução de rotinas e processos;
- Ataques de negação de serviço;
- Exploração de vulnerabilidades de protocolos;
- Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio de um gestor;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa, ou provedor de acesso.

Notificaremos por e-mail aos responsáveis pelo contrato em um prazo de até 24 (vinte e quatro) horas após o conhecimento de qualquer violação de segurança no âmbito das atividades do contrato.

Na notificação, informaremos:

> **(i)** data e hora do incidente; **(ii)** data e hora da ciência da empresa.; **(iii)** relação dos tipos de dados afetados pelo incidente; **(iv)** número de usuários afetados (volumetria do incidente) e, se possível, a relação destes indivíduos; **(v)** descrição das possíveis consequências do evento;

5. Ponto focal para acionamento em caso de questões envolvendo segurança e privacidade

Pelo e-mail: ocorrencias@emnuvens.com.br
Abertura de chamado: https://suporte.lepidus.com.br/ / suporte@lepidus.com.br

Responsáveis: Maria Mariana, Diego Abadan e Pablo Valério Polônia.

Contatos adicionais em: https://lepidus.com.br/contato/

6. Procedimentos para concessão de acesso ao ambiente *Open Journal Systems* (OJS)

Trabalhamos na modalidade SaaS, onde os usuários acessam a aplicação (OJS) através de sua interface Web e/ou sua API Web. Somente parte de nossa equipe técnica, vinculada à área de segurança e infraestrutura de tecnologia da informação, tem acesso aos servidores, logo, tendo acesso ao sistema operacional, código da aplicação, seus arquivos e base de dados.

Por segurança, hoje nenhum cliente tem acesso aos servidores (ex.: ssh/sftp) ou bases de dados, dada a política de menor privilégio para maior segurança e a garantia que o OJS fornecido é mantido por nossa equipe.

Os dados do OJS podem ser replicados automaticamente em um local de responsabilidade do contratante, permitindo assim o acesso independente pelo mesmo aos dados, devendo este se comprometer com a segurança, monitoramento e disponibilidade do mesmo. Alternativamente, o acesso a dados não fornecidos pela API do OJS podem ser fornecidos por outras formas como, por exemplo, a criação de um plugin que exponha os dados desejados em um formato pré-definido, perante negociação entre as partes.

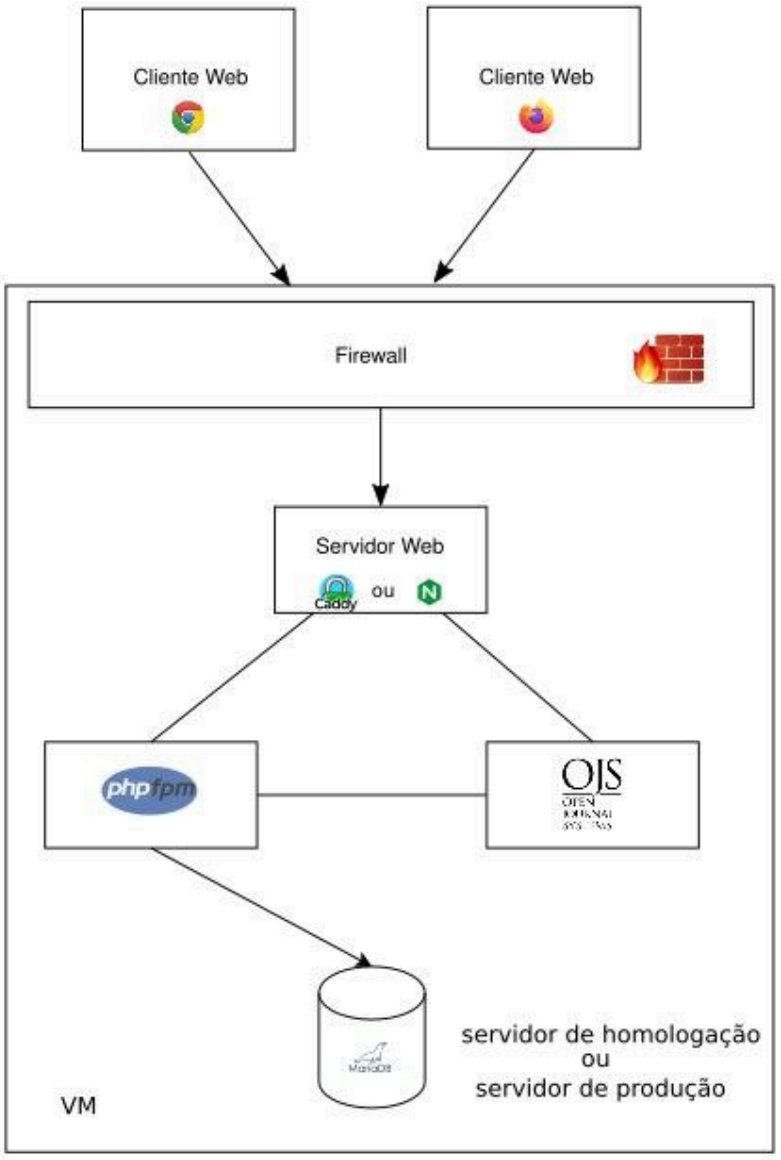
7. Entrega dos dados em caso de necessidade

Os dados são de propriedade da instituição contratante e podem ser solicitados sempre que necessário. Uma cópia periódica dos dados poderá ser armazenada na infraestrutura da instituição, de forma a haver autonomia e independência para consultas aos dados, devendo a periodicidade e modo de disponibilização dessas informações ser acordada por escrito entre as partes.

Em caso de rescisão contratual, os dados sob custódia da Lepidus são disponibilizados para o contratante pelo prazo definido em contrato. Esse prazo pode ser ampliado mediante solicitação prévia e está sujeito a cobrança de eventuais taxas de serviço.

8. Detalhamento da infraestrutura alocada:

O diagrama a seguir ilustra a arquitetura de hospedagem da maioria das instâncias OJS em nossos servidores.



9. Escolha de fornecedores:

Visando prover a maior disponibilidade e qualidade dos serviços trabalhamos com diversos provedores de infraestrutura. A escolha do fornecedor utilizado para hospedar determinado cliente é dinâmica, podendo ser alterada ao longo do tempo. Não temos exclusividade com um fornecedor, sendo que a manutenção da aplicação é feita exclusivamente por nossa equipe.

A contratação de um fornecedor leva em consideração a sua reputação, quando passa a ser permanentemente avaliado por nossa equipe quanto a qualidade do serviço, nos permitindo fornecer uma ótima experiência para o usuário final de nossas aplicações.

10. Gestão de vulnerabilidades

Como o OJS é um software livre, nossa equipe monitora as correções disponibilizadas pela fornecedora (PKP) e as aplica como remendo (*patch*) ou atualização de versão no menor tempo possível. Temos contato direto com a equipe de desenvolvimento da ferramenta OJS, onde podemos consultá-los sobre possíveis problemas de segurança e receber informações antecipadas sobre vulnerabilidades sendo tratadas ou investigadas.

Além disso, todos componentes que o OJS depende são atualizados automaticamente, sendo mantidos por fornecedores com boa reputação. Por exemplo, do kernel Linux ao PHP, utilizamos o software disponível pela distribuição GNU/Linux Ubuntu ou Debian* com suas atualizações de segurança instaladas automaticamente.

* Distribuições utilizadas no momento da confecção desse documento, podendo ser alteradas ao longo do tempo ou para casos/sistemas específicos.

11. Monitoramento

Nossos serviços são monitorados de forma permanente. A equipe técnica é notificada em casos de indisponibilidade, para que possa tomar as medidas necessárias. Os serviços de base de infraestrutura utilizados pelo OJS, como uso dos processadores e memória, conectividade de rede e base de dados também são monitorados.

12. SLA de tempo de serviço

Oferecemos um SLA *(Service Level Agreement*) de manutenção no ar do serviço por 99% do tempo, em cada mês civil, ressalvados o caso fortuito e a força maior ou nos casos de:

a. falha de conectividade decorrentes de falhas em operadoras de telecomunicações e rotas de comunicação com o centro de dados onde está hospedado o Periódicos em Nuvens não pertencentes à Lepidus;

b. falha na conexão de internet, sem responsabilidade da Lepidus;

c. falha em domínio ou DNS de responsabilidade do cliente;

d. intervenções emergenciais decorrentes da necessidade de preservar a segurança, implementar correções de segurança, evitar ou fazer cessar atividades maliciosas ou que prejudiquem o bom funcionamento do serviço;

e. suspensão da prestação dos serviços contratados por determinação de autoridades competentes, ou por descumprimento de cláusulas do contrato;

f. manutenções que possam demandar mais tempo de indisponibilidade, como uma atualização maior do OJS ou de sistemas que este dependa, desde que previamente agendadas com o cliente.

13. Recuperação dos dados em casos de incidentes

Em caso de incidentes de segurança, o cliente é avisado em até 24h após a sua descoberta, conforme detalhado no item 4.

O servidor onde a aplicação estava hospedada é considerado **comprometido**, deixando de ser utilizado imediatamente e passando por uma auditoria visando identificar a falha de segurança que permitiu o incidente.

Em paralelo, são restaurados os dados do cliente em um novo servidor com uma instalação limpa do sistema operacional, do Open Journal Systems e de suas dependências (PHP, banco de dados, etc), como a base de dados e arquivos submetidos (artigos, avaliações, imagens, etc), inspecionados e depois de validados, o serviço é restaurado.

O prazo para recuperação do OJS é de, no máximo, 72 horas.