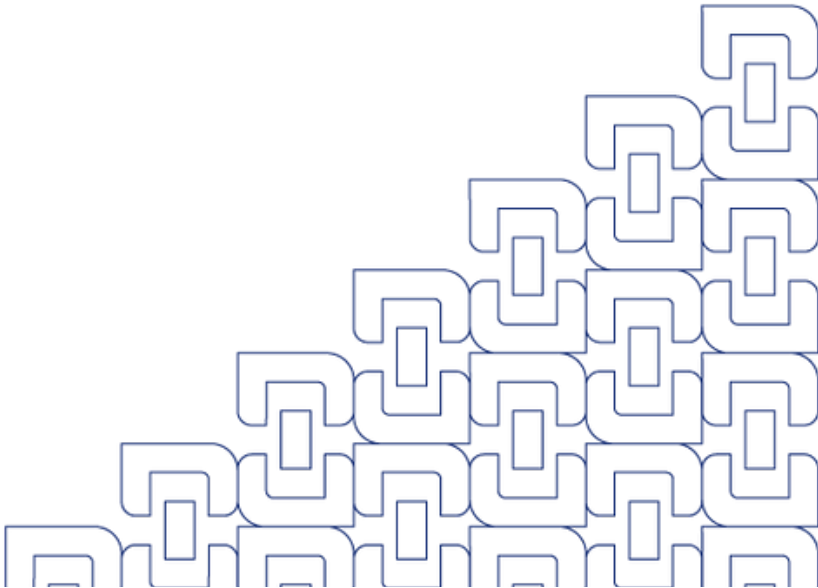
POLÍTICA DE SEGURANÇA

NURIA



Departamento que possui este documento	Segurança da Informação (SI)
Responsável pelo departamento	Lucas Belo Passos
Cargo:	CISO
Endereço de e-mail:	si@nuria.com.br
Telefone:	(31) 2535-4023

Versão	Revisado por	Data de Revisão	Aprovado por	Cargo do aprovador	Data aprovação
2.0	Yasmin Viola e Jonathan Pimenta.	13/04/2023	Lucas Passos	CISO	13/04/2023

A Segurança dos dados é importante para nós

Como especialistas em integração de sistemas da saúde, sabemos da responsabilidade que temos ao tratar as informações de nossos clientes e parceiros. Neste contexto, utilizamos um conjunto de boas práticas e políticas para garantir a proteção e a segurança dos dados.

Segurança de Infraestrutura

Utilizamos as boas práticas recomendadas e padrões para garantir a segurança e privacidade. A infraestrutura da NURIA se encontra na Amazon Web Services (AWS), que atende aos mais rígidos requisitos de segurança, os quais são auditados e certificados. Para obter mais detalhes sobre conformidade na AWS.

Conformidade e regulamentações

A NURIA tem apoiado seus clientes no atendimento da LGPD por trazer facilidade na governança de dados. Enquanto operadores de dados pessoais, garantimos segurança e eficiência na gestão. Além disso, a NURIA possui uma Política Interna de Proteção de Dados que faz parte do onboarding de todos os seus colaboradores e é periodicamente reforçada por meio de treinamentos.

LGPD – Nossas atividades estão em conformidade com a Lei Geral de Proteção de Dados, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Segurança em Nuvem

Segurança física – A NURIA tem toda infraestrutura na Amazon Web Services (AWS) que gerencia a segurança física e ambiental. A AWS possui recursos como fontes de energia de emergência, equipamento de supressão de incêndios, vigias, cercas, sistema interno de segurança entre outras medidas que podem ser analisadas com mais detalhes através do informativo das medidas de controle e segurança da AWS. Além disso, nosso programa de segurança interna cobre a segurança física em nosso escritório.

Segurança de infraestrutura – Os dados são hospedados nos data centers da AWS que atendem a normas como ISO 27001, PCI DSS, SOC 2 e outros. Para obter mais detalhes sobre conformidade na AWS.

Segurança de rede – Nossa rede é protegida com o uso dos principais serviços de segurança da AWS, auditorias regulares e monitoramento de rede. Para obter mais detalhes sobre a infraestrutura de segurança da AWS.

Disponibilidade e continuidade – A NURIA mantém monitoramento ativo 24/7 e melhores práticas de gestão de incidentes, além da página de status de disponibilidade do sistema e histórico de incidentes que pode ser acessado. Nosso programa de recuperação de desastres garante que nossos serviços permaneçam disponíveis e sejam recuperados rapidamente minimizando o impacto em um cenário de desastre.

Logs de ações e atividades – São mantidos logs de ações e atividades como modificação de configurações, criação e exclusão de ativos das assinaturas de produção para permitir auditorias e investigações sempre que necessário.

Monitoramento – Existe monitoramento de ações por meio de dashboard e alertas onde são inspecionadas o compliance do ambiente com relação às políticas de segurança em vigor.

Segurança da Aplicação

Desenvolvimento seguro (SDLC) – Além dos controles e testes executados durante o processo de implementação, desenvolvemos internamente a habilidade em desenvolvimento seguro. Para isso, promovemos treinamentos que incluem os 10 principais riscos de segurança da OWASP, vetores de ataque comuns e controles de segurança.

Segregação de ambientes – Existe a separação dos ambientes de desenvolvimento, homologação e produção, considerando para cada um suas respectivas permissões de acesso. O ambiente produtivo segue o conceito do mínimo privilégio e nenhum dado de produção é usado em nossos ambientes de desenvolvimento ou teste.

Execução de pentest – Realizamos, a cada ano, a contratação de empresa terceira independente para execução de pentest do tipo gray box.

Análise de código estático – SAST – Todo pipeline de compilação é examinado através de uma ferramenta de análise estática de código. Com esta ferramenta são avaliadas categorias de defeitos de software, entre eles: code smells, vulnerabilidades e security hotspots.

Análise SCA – Software Composition Analysis – É realizada a verificação de software componente, bibliotecas, e busca de vulnerabilidades.

Guarda de código fonte – Os códigos fontes são armazenados em repositório Git privado, com acesso autorizado utilizando autenticação integrada.

Gestão de segredos – Informações sensíveis de aplicativos como chaves de API e senhas de bancos de dados são armazenadas em cofre de senha com log de atividade e acesso restrito de rede.

Equipe de segurança dedicada – Nossa equipe de segurança está disponível para responder a alertas e eventos de segurança.

Segurança do Produto

Controle de acesso – Controle de acesso granular baseado em funções com níveis de permissão, seguindo o modelo RBAC, com a possibilidade de integração com SSO para autorização, além de autenticação.

Restrições de IP – As aplicações da NURIA podem ser configuradas, no contexto de integrações, para permitir o acesso à API, somente de intervalos de endereço IP específico podem ser configuradas, no contexto de integrações, para permitir o acesso à API, somente de intervalos de endereço IP específicos definidos.s definidos.

Resposta a incidentes de segurança – Em caso de incidente de segurança, o time responsável pela gestão de incidentes é acionado. Esta equipe é treinada em processos de resposta a incidentes de segurança, com o objetivo de aplicar ações rápidas para minimizar impactos.

Segurança dos Dados

Criptografia – Usamos padrões de criptografia fortes para proteger os dados em trânsito entre os clientes da NURIA e o provedor de serviços de nuvem AWS e em repouso.

Criptografia de dados em trânsito – Toda a comunicação com a interface e as APIs da NURIA é criptografada pelo padrão HTTPS/TLS (TLS 1.2 ou posterior) em redes públicas.

Criptografia de dados em repouso – Os dados são criptografados em repouso na AWS usando o algoritmo criptográfico AES-256

Análise de código estático – SAST – Todo pipeline de compilação é examinado através de uma ferramenta de análise estática de código. Com esta ferramenta são avaliadas categorias de defeitos de software, entre eles: code smells, vulnerabilidades e security hotspots.

Análise SCA – Software Composition Analysis – É realizada a verificação de software componente, bibliotecas, e busca de vulnerabilidades.

Guarda de código fonte – Os códigos fontes são armazenados em repositório Git privado, com acesso autorizado utilizando autenticação integrada.

Gestão de segredos – Informações sensíveis de aplicativos como chaves de API e senhas de bancos de dados são armazenadas em cofre de senha com log de atividade e acesso restrito de rede.

Equipe de segurança dedicada – Nossa equipe de segurança está disponível para responder a alertas e eventos de segurança.

Segurança do Produto

Controle de acesso – Controle de acesso granular baseado em funções com níveis de permissão, seguindo o modelo RBAC, com a possibilidade de integração com SSO para autorização, além de autenticação.

Restrições de IP – As aplicações da NURIA podem ser configuradas, no contexto de integrações, para permitir o acesso à API, somente de intervalos de endereço IP específicos definidos.

Resposta a incidentes de segurança – Em caso de incidente de segurança, o time responsável pela gestão de incidentes é acionado. Esta equipe é treinada em processos de resposta a incidentes de segurança, com o objetivo de aplicar ações rápidas para minimizar impactos.

Segurança dos Dados

Criptografia – Usamos padrões de criptografia fortes para proteger os dados em trânsito entre os clientes da NURIA e o provedor de serviços de nuvem AWS e em repouso.

Criptografia de dados em trânsito – Toda a comunicação com a interface e as APIs da NURIA é criptografada pelo padrão HTTPS/TLS (TLS 1.2 ou posterior) em redes públicas.

Criptografia de dados em repouso – Os dados são criptografados em repouso na AWS usando o algoritmo criptográfico AES-256.

Backups – Os backups são diários e automatizados (RDS) e versionamento (S3). Monitoramos toda a infraestrutura de forma ativa para a detecção de anomalias, via CloudWatch. São aplicados fortes controles de proteção de backup e realizados testes de restore.

Localização de armazenamento dos dados – As aplicações e dados da NURIA estão hospedados nos servidores da Amazon Web Services (AWS), localizados na região sa-east-1 (São Paulo – Brasil).
A Amazon possui vários programas de conformidade relacionados à segurança, como a ISO 27001, PCI nível 1, HIPAA e SOC.

Segurança em Recursos Humanos

Cultura e conscientização – Nosso programa de cultura e conscientização tem como objetivo treinar todos os colaboradores da NURIA e fazer com que pensar sobre Segurança da Informação se torne naturalmente parte do dia a dia. Para isso, contamos com o processo de onboarding, em que novos colaboradores são treinados pelo time de Segurança da Informação antes de iniciarem suas atividades, para conhecerem a Política da Segurança da Informação (PSI), Lei Geral de Proteção de Dados (LGPD) e outros tópicos.

Os times recebem rotineiramente, do time de Segurança da Informação, treinamentos a respeito de temas ligados à segurança e privacidade, em que são utilizados os canais de comunicação interna da NURIA para manter todos os colaboradores informados sobre temas relacionados à segurança, buscando a conscientização e que se mantenham atualizados a respeito da Política da Segurança da Informação (PSI).

Comitê de segurança da informação e conformidade – Possuímos um Comitê de Segurança da Informação e Conformidade com a participação de pessoas de diversos times, com o objetivo de identificação de necessidades de segurança, para uma ação proativa frente a possíveis riscos aos projetos bem como discussão de ações internas de Segurança da Informação na NURIA.

Links Úteis

Links de informações complementares
Conheça o CM Connect
Arquitetura e Conformidades
Política de Privacidade

A NURIA conta com um comitê de segurança da informação e privacidade para apoio nos direcionamentos relacionados à privacidade dos dados. Questões relacionadas à privacidade dos dados podem ser encaminhadas ao endereço eletrônico: dpo@nuria.com.br