



Política de Segurança Cibernética

Nós, da Rodobens, sabemos que parte importante da excelência de nossos serviços é a proteção de dados e informações relativas aos nossos Clientes, às nossas operações e aos nossos sistemas internos. Neste sentido, tomamos precauções, dentro dos mais altos padrões comerciais, a fim de garantir a segurança de tais dados e informações, respeitando, ainda as leis e normas aplicáveis a nossas atividades, adotando, ainda, padrões de segurança iguais ou superiores aos adotados no mercado.

A nossa Política de Segurança Cibernética ("Política") foi desenhada tendo em vista tais cuidados. Esta tem como objetivo transmitir os princípios de Segurança Cibernética que guiam nosso trabalho e os mecanismos de controle utilizados tanto para a prevenção como para o combate e tratamento de eventuais incidentes de Segurança Cibernética.

Assim, a fim de esclarecer para Você, nosso cliente, as condições de nossa Política de Segurança Cibernética, o presente documento apresenta um resumo dos principais pontos de tal documento.

I. Nossa Política de Segurança Cibernética

A nossa Política foi especificamente estruturada em concordância com o nosso porte, perfil de risco e modelo de negócio, assim como a complexidade dos nossos produtos, serviços, atividades e processos de instituição. Esta é aplicável a nossos colaboradores e prestadores de serviços, abrangendo todos os níveis hierárquicos.

II. Medidas de Segurança e Prevenção

A. Classificação dos Dados: Classificamos os dados em níveis de confidencialidade, de acordo com a natureza e a criticidade das informações tratadas, restringindo os níveis de acesso e reforçando os mecanismos de controle e segurança de acordo com a criticidade e sensibilidade de cada dado.

B. Equipamentos e Estrutura: Os equipamentos utilizados para o desenvolvimento das atividades da Rodobens devem estar sempre atualizados, regra que inclui sistema operacional, antivírus e *firewalls*, garantindo assim maior proteção às informações neles inseridas. Ainda, os cuidados se estendem também à infraestrutura onde são armazenados os dados: estes são criptografados e possuem cópias de segurança (*backups*) atualizadas periodicamente, conforme os padrões de segurança mais altos disponíveis no mercado.

C. Processamento, Armazenamento de Dados e Computação em Nuvem: Os serviços relevantes de armazenamento de dados e computação em nuvem que contratamos passam por uma seleção interna rígida, sendo amparada pelos seguintes critérios: (i) confirmação da capacidade técnica do prestador de serviço de cumprir o quanto disposto na Política e na legislação aplicável à segurança cibernética, por meio de auditoria ou da apresentação de declarações e/ou certificações pelo prestador de serviço; (ii) dificuldade ou impossibilidade técnica ou custo elevado para a execução do serviço relevante pela Rodobens em sua própria infraestrutura e (iii) a criticidade e relevância do serviço a ser contratado. Ainda, são cumpridos todos os requisitos previstos na regulamentação específica, em especial a Resolução nº 4.658/2018 do Conselho Monetário Nacional.

D. Obtenção de Credenciais e Gerenciamento de Acesso: Os nossos colaboradores e prestadores de serviço assumem rígidos compromissos de confidencialidade ao obterem as credenciais que dão acesso aos nossos dados confidenciais ou a dados classificados como sensíveis pela Rodobens. Estas credenciais, por sua vez, são atualizadas periodicamente, em conformidade com as regulações e normas aplicáveis. Ainda, o acesso aos dados é restringido a menor permissão e privilégio possíveis, possuindo a Rodobens capacidade para monitorar e registrar o acesso a dados classificados como sensíveis, sendo exigida a mesma garantia de seus prestadores de serviço.

E. Capacitação e Atualização: Os nossos colaboradores passam por periódicos cursos de capacitação referentes à prevenção e resposta a incidentes, bem como de melhores práticas de segurança cibernética, sendo realizadas ainda, avaliações



Política de Segurança Cibernética

buscando atingir o maior comprometimento de todos os nossos colaboradores. Além disso, disponibilizamos canais internos pelos quais os colaboradores possam encaminhar denúncias e suspeitas de fragilidades e violações de segurança cibernética, a fim de agilizar, assim, a resposta do time especializado a eventuais incidentes.

III. Respostas a Incidentes e Continuidade dos Negócios

Visando garantir a continuidade de nossas atividades em caso de eventuais incidentes de segurança cibernética, realizamos, constantemente, testes de continuidade de negócios, nos seguintes cenários:

- Exploração de possíveis vulnerabilidades que permitam o acesso, a cópia e /ou a extração de informações e dados internos e/ou confidenciais do ambiente lógico da Rodobens;
- Realização de testes de intrusão a base de dados contendo informações sensíveis da Rodobens;
- Tempo de recuperação de acesso a informações de backup em caso de perda de Informações sensíveis;
- Estratégias para a recuperação de informações sensíveis e serviços relevantes.

Assim, após a identificação de possíveis fragilidades efetuamos todas as adequações e alterações necessárias para que a nossa segurança seja mantida.

IV. Contato

Quaisquer dúvidas ou sugestões são bem-vindas e podem ser encaminhadas para nós por meio do e-mail: protecaodedados@rodobens.com.br