Riscos Emergentes

Informe Temático

Na TIM, o processo ERM (Enterprise Risk Management) é iniciado anualmente pelo presidente do Steering Committee ERM, a partir da comunicação adequada, com objetivo de avaliar o perfil de risco e monitorar a sua evolução. É um processo cíclico, que deve estar coerente com o plano industrial, definido nas seguintes fases:

Definição do Risk Appetite e Risk Tolerance: auxiliar o management na definição e estruturação do valor de apetite ao risco, aceitável pela companhia para o ano vigente, bem como na definição e acompanhamento dos indicadores de tolerância ao risco, alinhados com os objetivos estratégicos predefinidos no Plano Industrial.

Risk Assessment: identificação e avaliação dos riscos que possam impactar o atingimento dos objetivos do plano, com foco particular sobre os objetivos que foram definidos para o Risk Tolerance. Os riscos devem ser identificados a partir das entrevistas com os Process Owners e avaliados de acordo com dois direcionadores: Nível de Risco Inerente e Nível de Monitoramento, consequentemente, sendo posicionados no Risk Control Panel.

Risk Response: identificação e implementação de ações de mitigação e, de forma geral, resposta ao risco, cuja avaliação foi realizada na fase de Risk Assessment. As fases do Risk Response são: i) planejamento, ii) execução, iii) avaliação final e mensuração de performance.

Monitoramento, Controle e Avaliação de Performance: monitoramento e análise da evolução de cada risco, das relativas ações de mitigação, perfil global de riscos resultante e das atividades de monitoramento do atingimento dos objetivos definidos no Risk Appetite e Risk Tolerance.

A TIM executa análises de sensibilidade ou testes de estresse sobre riscos financeiros e/ou não financeiros periodicamente. Além disso, revisamos anualmente a exposição ao risco de nossa empresa seguindo as fases acima relacionadas e submetemos nossos processos de gerenciamento de risco a auditorias internas e externas.

Eventos podem ter impacto negativo, positivo, ou, até mesmo, ambos. Os eventos cujo impacto é negativo representam riscos, exigindo avaliação e resposta da administração, de forma a não prejudicar a realização dos objetivos. Eventos cujo impacto é positivo representam oportunidades, possibilitando influenciar favoravelmente na realização dos objetivos, apoiando a criação de valor. Os eventos que neutralizam o impacto negativo dos riscos são levados em conta na avaliação de riscos e resposta a estes.

Eventos externos novos, com impactos significativos de curto ou longo prazo também são avaliados de forma a preparar a empresa para responder ao risco, seja adaptando-se, seja criando as condições para que o risco não se materialize ou seja mitigado. Os riscos emergentes a seguir fazem parte dessa análise e seus impactos esperados foram baseados no Relatório de Riscos Globais do Fórum Econômico Mundial e no relatório Top Emerging Risks da KPMG.

Falha na Ação Climática

Título do risco (Nome): Falha ou execução inadequada na prestação de serviços devido a eventos climáticos extremos (Mudanças Climáticas).

Categoria: Estratégico / Ambiental

Descrição do risco: Não executar plano estratégico de ESG e nem contribuir para a redução das emissões de GEE (causa do aumento do aquecimento global e eventos climáticos extremos mais frequentes que podem afetar a disponibilidade de serviços de telecomunicações), não cumprir os compromissos assumidos ao mercado (redução de emissões de GEE, carbono neutro, SBTi), gerando efeitos negativos em termos de finanças, conformidade, reputação de marca e satisfação do stakeholder. Falha no planejamento e execução das ações de adaptação da empresa às mudanças climáticas (por exemplo, redução do consumo de energia elétrica, identificação de vulnerabilidades a eventos climáticos extremos, continuidade de negócios).

Riscos emergentes associados: *Falha na ação climática.* Falha em impor, promover ou investir em medidas eficazes de adaptação e mitigação das mudanças climáticas, preservar ecossistemas, proteger populações e fazer a transição para uma economia neutra em carbono.

O não cumprimento das medidas necessárias sobre as mudanças climáticas globais intensificará a ocorrência de condições climáticas extremas, incluindo enchentes e tempestades inesperadas. O aumento da ocorrência dessas condições climáticas extremas, tem o potencial de danificar, por exemplo, as estruturas (como antenas) necessárias para a distribuição do sinal de telecomunicações, o que pode interromper o serviço e criar dificuldades para restaurá-lo.

As informações sobre nossa vulnerabilidade podem não ser precisas, considerando que operamos em uma ampla distribuição geográfica. Riscos climáticos imprevistos podem ocorrer e podemos não estar preparados para esses efeitos fazendo a transição no momento certo. Podemos ser impactados de várias maneiras: seja por não alocar nossos ativos em locais apropriados e seguros, seja por não fazer a transição de nossas redes para operar com fontes de energia com menor probabilidade de serem afetadas.

A empresa conta com energia elétrica predominantemente hidrelétrica, vulnerável a mudanças nos padrões climáticos. Muitas empresas buscarão a transição de sua fonte de energia criando uma alta demanda por alternativas de eletricidade. Portanto, a empresa depende de mudanças na infraestrutura regional que estão além do alcance da empresa para mudar.

O risco e seu impacto na empresa são específicos: a empresa deve prestar serviços onde os clientes estão localizados, e uma falha no rastreamento da migração humana devido às mudanças climáticas pode afetar nossa capacidade como prestadora de serviços de identificar as necessidades dos clientes. Além disso, a sede da empresa e seu centro de desenvolvimento tecnológico está localizada na zona litorânea do Rio de Janeiro, onde a elevação do nível do mar

pode causar grandes danos, incluindo comprometimento do serviço e falha na proteção de nossos funcionários.

Impacto: A distribuição generalizada em todo o país dos ativos da TIM é necessária para a realização de seus negócios, todavia, expõe a empresa a possíveis danos físicos diretos e indiretos decorrentes desses eventos climáticos, que podem comprometer a qualidade e a integridade de nossos serviços.

Considerações de gestão (Ações mitigadoras): Nosso plano estratégico ESG foi projetado para contribuir para a redução das emissões de GEE (causa do aumento do aquecimento global e eventos climáticos extremos mais frequentes que podem afetar a disponibilidade de serviços de telecomunicações), para cumprir os compromissos assumidos com o mercado (redução das emissões de GEE, neutra em carbono, SBTi) e ajudar as comunidades a serem resilientes em incidentes climáticos extremos. Essas ações também contribuem para evitar a geração de efeitos negativos em termos de finanças, compliance, reputação da marca e satisfação das partes interessadas.

Nossos projetos de geração distribuída de energia renovável e os projetos SKY Coverage e RAN Sharing permitirão que a TIM reduza suas emissões a partir da redução do consumo de energia, aumento de eficiência e a autogeração de energia renovável. Além disso, visando mitigar os riscos físicos das mudanças climáticas, avaliamos continuamente a resiliência das nossas instalações buscando identificar vulnerabilidades. Mais informações sobre riscos relacionados às mudanças climáticas e nossas estratégias de mitigação e adaptação podem ser encontradas no Informe Temático – Mudanças Climáticas.

Falha nas medidas de segurança cibernética

Título de risco (Nome): Gerenciamento ineficiente dos processos preventivos de ataques cibernéticos

Categoria: Estratégica / Tecnológica

Descrição de risco: O processo de prevenção a ataques cibernéticos não estar adequado, causando exposições à empresa, permitindo possíveis ataques que visam comprometer a infraestrutura de rede/dispositivos corporativos ou adquirir informações/dados, também em referência à introdução de novas tecnologias (por exemplo, nuvem móvel, mídia social, big data, etc.)

Riscos emergentes associados: *Falha nas medidas de segurança cibernética*. As medidas de infraestrutura e proteção de segurança cibernética podem ser superadas ou tornadas obsoletas por crimes cibernéticos cada vez mais sofisticados e frequentes.

As operações e o negócio da companhia estão intrinsicamente relacionados com a transmissão de informações e o meio digital. No contexto de dependência generalizada de sistemas digitais cada vez mais complexos, as ameaças cibernéticas crescentes estão superando a capacidade das sociedades de preveni-los e gerenciá-los efetivamente.

Ataques cibernéticos são externos à companhia e podem ter origens variadas e podendo afetar a companhia e seus negócios de maneiras diversas: decorrente de tensões políticas (acesso aos sistemas para transmissão de informações políticas, ou para prejudicar movimentos políticos), movimentos sociopolíticos (como intenção de invadir para obter acesso a dados específicos, para fragilizar empresas do setor de telecomunicações ou mesmo transmitir mensagens por meio dos sistemas da companhia) ou mesmo como consequência indireta de riscos macroeconômicos (como a deterioração de condições econômicas no país que levam mais pessoas a buscarem meios de lucrar de maneira ilícita, dentre elas a venda de dados).

No contexto da pandemia, a segurança cibernética ganhou ainda mais relevância para manter as informações dos clientes seguras e proteger contra danos e possíveis interrupções dos serviços críticos.

O risco e os impactos são específicos para a companhia na medida em que como empresa de telecomunicações nossos sistemas são vias particularmente importantes para operacionalizar ataques e nossas bases de dados de clientes compreendem uma parcela significativa de pessoas. E a companhia está aprimorando meios de prevenir a materialização do risco e mitigar impactos.

Com um olhar de longo prazo, analisamos que há aspectos da LGPD (Lei Geral de Proteção de Dados) que entrarão em vigor e que ainda não é claro como a ANPD (Autoridade Nacional de Proteção de Dados) vai aplicar multas por violações no tratamento de dados, ainda não existem precedentes ou um guia como o elaborado pelo European Data Protection Board. Portanto, é um risco emergente pois a autoridade de dados brasileira ainda está se estabelecendo as regras, sendo

esperado a aplicação de multas. Na ausência de normas de dosimetria pode-se ter aplicação desigual.

Impacto: As violações de segurança cibernética podem causar vazamento de dados, expondo dados pessoais e sensíveis dos clientes, informações estratégicas dos negócios e indisponibilidade dos serviços críticos. Também pode afetar a disponibilidade de serviços para clientes, perda financeira e interrupção de cadeias de suprimentos críticas. A imagem, a reputação e os principais clientes da TIM também podem ser afetados, podendo resultar em instabilidade econômica e social.

Considerações de gestão (Ações mitigadoras): A TIM realiza suas atividades de Cybersecurity com base na ISO 27001/2013 - norma internacional que descreve as melhores práticas para gestão da segurança da informação e NIST (Cyber Security Framework), em apoio à gestão e buscando a redução dos riscos de segurança da informação. Nesse processo, desde 2017, a TIM implementou ferramentas e mecanismos de proteção para prevenir ataques cibernéticos, oferecendo soluções e produtos de baixo custo para melhorar a proteção de dados para nossos clientes e outros negócios. Nesse sentido, a TIM melhora continuamente a Filtragem de Acesso à Rede, adota o Anti-DDOS, possui um serviço de inteligência de ameaças, realiza varreduras para vulnerabilidades em andamento em escala, usa uma Plataforma de Divulgação Responsável (Bug Bounty) e implementou procedimentos de controle e investimentos em equipes de prevenção, tratamento de incidentes e monitoramento. Estamos usando o CIS Controls (Centre for Internet Security Controls) para implantar as melhores práticas que organizam medidas de segurança cibernética. A TIM promove testes independentes por funções no 2º nível de controle (Compliance Tecnológico).

Os processos de cybersecurity estão cada vez mais sendo fortalecidos, consolidados e gerenciados, apoiados pelas soluções mais modernas para garantir as melhores proteções de segurança, com ações preventivas de monitoramento e resposta, a fim de minimizar e impactar os clientes da TIM. Com isso, em 2022 a TIM obteve a certificação internacional ISO 27001, meta realizada prevista no seu Plano ESG.

Coordenação de RSC da TIM

Regulatory, Institutional and Press Relations – Environmental, Social & Governance – Responsabilidade Social Corporativa

respsocialcorp@timbrasil.com.br