Data da última atualização: 23/08/2021.

Política de Segurança da Informação e Segurança Cibernética

INTRODUÇÃO

As empresas do Grupo TIM no Brasil buscam constantemente prevenir e proteger todos os seus ativos, inclusive de ataques cibernéticos, através dos fundamentos da segurança cibernética no âmbito das redes e serviços de telecomunicações e da mitigação de riscos em infraestruturas críticas, assegurando os princípios de autenticidade, confidencialidade, disponibilidade, diversidade, integridade, interoperabilidade, prioridade, responsabilidade e transparência.

A proteção da informação, incluindo dado pessoal e dado pessoal sensível, além de todos os ativos a ela relacionados, é um elemento fundamental para garantir o controle estratégico dos riscos de segurança da informação e segurança cibernética, orientado aos interesses e resultados das empresas do Grupo TIM no Brasil e de seus usuários, guardando relação com a capacidade da empresa de enfrentar crises, proteger pessoas, ativos, instalações, informações, sistemas e operações.

O tratamento dos dados pessoais é realizado de maneira ética e responsável em respeito à Lei Geral de Proteção de Dados, conforme boas práticas e diretrizes estabelecidas na Política de Privacidade, publicada no Web Site da TIM, disponível no endereço https://www.tim.com.br/.

OBJETIVO

O objetivo deste documento é definir as diretrizes quanto à segurança da informação e segurança cibernética, no âmbito das redes e serviços de telecomunicações, incluindo também a proteção das infraestruturas críticas de telecomunicações das empresas do Grupo TIM no Brasil.

DESTINATÁRIO

As políticas de segurança da informação e segurança cibernética se aplicam a todos os colaboradores e fornecedores ou parceiros comerciais das empresas do Grupo TIM no Brasil, inclusive o Instituto TIM.

Este extrato das políticas de segurança da informação e segurança cibernética se destina aos clientes, de forma a demonstrar as medidas de segurança realizadas pelas empresas do Grupo TIM no Brasil, para garantir a continuidade na prestação dos serviços e na proteção dos seus dados.

REFERÊNCIAS

- ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- NIST (National Institute of Standards and Technology);
- Resolução Anatel Nº 740, de 21 de dezembro de 2020;
- Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018;
- Glossário de Segurança da Informação (Portaria nº 93/2019);
- Política de Privacidade TIM;
- Esta política é complementada por documentos normativos internos e específicos de segurança da informação e segurança cibernética das empresas do Grupo TIM no Brasil, em conformidade com os aspectos legais e regulamentares e aprovados pela alta administração.

As referências nacionais e internacionais são revisadas rotineiramente, de forma a garantir a adoção das melhores práticas em segurança.

RESPONSABILIDADES

A diretoria Cyber & ICT Security é responsável por assegurar as atividades de planejamento e controles de segurança, processos relativos à identificação e tratamento dos riscos, monitoramento das redes e serviços de telecomunicações, o gerenciamento dos incidentes de segurança, com foco no acompanhamento das ameaças, bem como a condução das atividades relativas à continuidade do negócio, baseando-se em normas, padrões, melhores práticas de mercado e documentos normativos de segurança internos da TIM.

Responsável por esta política: Claudio Creo, diretor Cyber & ICT Security.

CONTATO

Canal de comunicação disponível para o caso de eventuais urgências: csoc@timbrasil.com.br.

AÇÕES DE CONSCIENTIZAÇÃO

É prevista a definição de políticas e a implementação de procedimentos organizacionais, com o objetivo de conscientizar, disseminar, coordenar e monitorar o programa de gerenciamento de riscos de segurança da informação, contemplando a segurança cibernética.

Campanhas de conscientização e educação sobre aspectos de segurança da informação e segurança cibernética são realizadas para garantir o alinhamento com as políticas e diretrizes da empresa. Ações realizadas buscam treinar o colaborador, fornecedor ou parceiro comercial para diversas situações que envolvam riscos e ameaças à segurança. Como exemplo de ações preventivas: campanhas periódicas de comunicação, simulações de ataques cibernéticos e planos de ação para disseminação e conscientização da segurança da informação.

A TIM realiza, sempre que necessário, campanhas de conscientização com seus clientes, sobre aspectos da segurança da informação e segurança cibernética, buscando evitar possíveis riscos e ameaças, garantindo assim a segurança, a confiança e o bem-estar dos seus clientes. Como exemplo, cita-se o link sobre "dicas de segurança" presente no Web Site da TIM, disponível em: https://site.tim.com.br/sp/sobre-a-tim/institucional/seguranca/dicas-de-seguranca.

NOTIFICAÇÕES DE INCIDENTES DE SEGURANÇA CIBERNÉTICA

A diretoria Cyber & ICT Security é responsável pelo mapeamento e identificação de possíveis riscos de eventos e incidentes que possam afetar, de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários. Devem ser compartilhadas informações referentes a incidentes relevantes e outras informações relativas à segurança cibernética, incluindo análise de causa e do impacto, bem como ações mitigatórias adotadas, conforme definido nas legislações e regulamentações vigentes sobre o tema.

PRINCIPAIS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

No âmbito das redes e serviços de telecomunicações e da mitigação de riscos de segurança da informação e segurança cibernética são relacionados os principais processos abaixo:

- **Gestão de Ativos:** É parte fundamental para o gerenciamento da segurança da informação e segurança cibernética.

  Os Ativos TIC são configurados, conforme padrão pré-estabelecido, licenciados e homologados, além disso são atribuídos a um responsável, são inventariados e classificados, de acordo com sua criticidade;

- **Governança:** Gerenciamos as políticas, demais documentos normativos operacionais e indicadores para monitoramento e avaliação da aplicação dos requisitos de segurança, garantindo a conformidade com o ciclo de vida da informação;

- **Gestão de Riscos:** Realizamos a identificação e análise de risco definida com base nos objetivos de segurança, nos impactos nos negócios causados por incidentes de segurança, na probabilidade de ocorrência de incidentes de segurança e no nível de exposição para ameaça;

- **Gestão de Riscos em Fornecedor ou parceiro comercial:** Fazemos a avaliação com foco na adequação aos requisitos de segurança recomendados em contrato, acordando a

confidencialidade, para quem presta serviço, fornece produto e equipamento de telecomunicações;

- **Gestão de Acesso:** Apenas usuários autorizados possuem acesso à informação e instalações, devendo essa autorização ser aprovada pelo responsável, inibindo desta forma o acesso indevido.
    - **Acesso Lógico:** Utilizamos o princípio de "Mínimo Acesso Necessário" e "Segregação de Função", de acordo com função e responsabilidade para o desempenho da tarefa atribuída;
    - **Acesso Físico:** Garantimos a prevenção de danos às instalações, a integridade dos ativos, inclusive das infraestruturas críticas. As áreas devem ser projetadas para minimizar os riscos de acesso de pessoal não autorizado.
- **Classificação da Informação:** Disponibilizamos campanhas e ferramentas para classificação da informação, orientando que toda a informação gerada, no âmbito da empresa, deve ser classificada pelo seu proprietário quanto à sua confidencialidade e protegida durante todo o seu ciclo de vida. Os tipos de classificação previstas são: Público, Uso Interno, Confidencial ou Exclusivo;
- **Desenvolvimento Seguro:** Avaliamos a segurança do código fonte dos Ativos TIC, com o objetivo de prevenir prejuízos que possam ocorrer por falhas de segurança;
- **Gestão de Log:** Asseguramos a rastreabilidade das ações realizadas pelos usuários nos Ativos TIC das empresas do Grupo TIM no Brasil, através de registros e monitoramentos, a fim de garantir possível detecção de ações impróprias, preservando a informação confidencial das ações realizadas, sendo armazenado pelo período mínimo necessário para sua finalidade;
- **Gestão de Criptografia:** Buscamos a proteção da informação, contra o acesso indevido, tornando-a confidencial, autêntica e sem repúdio, de forma a manter a privacidade, anonimato e segurança da transmissão;
- **Hardening e Patch:** Implementamos configurações seguras e realizamos atualizações para redução de exposição dos ataques ao Ativo TIC, inclusive infraestruturas críticas que possam comprometer os pilares de segurança da informação;
- **Gestão de Backup e Restore:** Realizamos armazenamento e recuperação da informação e/ou dados, com a finalidade de manter a informação disponível, quando na ocorrência de algum evento com impacto, por exemplo: desastres naturais, falhas em sistema de disco, sabotagem, erro de entrada de dados, falha de sistema operacional, falha humana e solicitações jurídicas e entre outros;
- **Proteção de Perímetro:** Protegemos a infraestrutura, por meio de ferramentas padrão de mercado, realizando a detecção e resposta contra quaisquer tentativas de invasões, ataques de vírus, todo tipo de Malware malicioso, Spam, Phishing, ataques de DDoS e Scan externos. Utilizamos as ferramentas, mas não nos limitando a: Firewall, IPS, IDS, WAF, Antimalware e entre outros, para mitigação de vazamento de informações através de ferramentas preventivas

instaladas em dispositivos móveis, estações de trabalho, em contas de e-mails corporativos, WEB, impressão, além do uso de criptografia para dados em repouso e em transporte;

- **Prevenção ao vazamento de informações:** Utilizamos um conjunto de ferramentas e processos, que visa a proteção das informações sob custódia da empresa, garantindo a confidencialidade, integridade e disponibilidade dos dados em todo o seu ciclo de vida;
- **Avaliação de Vulnerabilidade:** Mitigamos os riscos de exposição cibernética, por meio da análise de vulnerabilidades e de testes de invasão, que buscam identificar, analisar e explorar as ameaças e os riscos associados à segurança cibernética nos Ativos TIC, inclusive nas infraestruturas críticas de telecomunicações das empresas do Grupo TIM no Brasil, garantindo a continuidade dos serviços de telecomunicações;
- **Monitoramento da evolução e a detecção de novas ameaças:** Avaliamos ameaças novas e as já existentes no espaço cibernético, através de pesquisas, a fim de mitigá-las com antecedência, evitando impactos na operação da empresa e para os clientes;
- **Investigação digital:** Analisamos os dados oferecidos em processos que possam sugerir a violação da legislação vigente e confrontamos com as evidências disponibilizadas pelos canais de denúncia;
- **Monitoramento e Tratamento de Incidentes:** Mapeamos possíveis riscos, registro de evento e tratamento de incidente tecnológico de segurança, garantindo uma resposta a incidente tecnológico de segurança e privacidade, de forma eficaz e eficiente, mitigando o nível aceitável do impacto do incidente, com possível prejuízo de impacto ao serviço, à imagem, à receita, ao negócio, à infraestrutura e ao cliente;
- **Gestão de Continuidade do Negócio:** Mantemos a disponibilidade dos produtos, serviços, atividades e processos mais críticos diante de incidentes e crises corporativos que possam causar impactos significativos aos objetivos de negócio das empresas do Grupo TIM no Brasil.

CONTROLES INTERNOS

A diretoria de Cyber & ICT Security está sujeita a controles internos sob a responsabilidade das diretorias Auditoria e Compliance, conforme documentos normativos publicados internamente.

COMITÊS DE MONITORAMENTO (Executivos e Operacionais)

- **Cyber & ICT Security Steering Committee:** Acompanhamento executivo de projetos e resultados relacionados à segurança cibernética das empresas do Grupo TIM no Brasil;
- **Comitês Operacionais de Tecnologia:** Comitês mensais de acompanhamento operacional dos projetos de segurança cibernética executados pelas diretorias tecnológicas.

GLOSSÁRIO

- **ANATEL:** Agência Nacional de Telecomunicações, autoridade reguladora do setor de telecomunicações no Brasil, com competências definidas pela Lei nº 9.472/97.
- **Ativo TIC (Tecnologia da Informação e Comunicação):** Tecnologias que permitem ao usuário acessar, armazenar, transmitir e manipular informações, tais como, mas não se limitando a: elementos de rede, sistemas, ativos de telecomunicações, entre outras ferramentas que venham a ser utilizadas no futuro em virtude da inovação tecnológica.
- **Grupo TIM no Brasil:** São as seguintes empresas: TIM Brasil Serviços e Participações S.A., e TIM S.A., bem como qualquer outra empresa que venha a ser parte do grupo via fusão ou aquisição ao longo da vigência da presente Política.
- **Incidente:** Evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
- **Infraestruturas Críticas de Telecomunicações:** Instalações, serviços, bens e sistemas, afetos à prestação de serviços de telecomunicações, que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.
- **Segurança Cibernética:** Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.
- **Segurança da Informação:** Ações que objetivam viabilizar e assegurar a confidencialidade, integridade, disponibilidade, autenticidade e a legalidade das informações.

Aprovado pelo Conselho de Administração em 26 de julho de 2021.