NORMATIVA SOBRE SEGURANÇA CIBERNÉTICA

SUMÁRIO:

RESPONSÁVEL E APROVADORES:

Área Responsável	Governança CTIO
Aprovadores	Infraestrutura e Segurança em TI, NOC, Site Management

1. OBJETIVO

Considerando que:

i. A FIBRASIL é autorizada a prestar o Serviço de Comunicação de Multimídia - SCM, de acordo com o Ato de Autorização ANATEL nº 7.820/2020;

ii. A FIBRASIL atua na prestação de serviço de exploração industrial de rede FTTH neutra, prestando seus serviços exclusivamente para outras empresas prestadores de serviços SCM que a exploram industrialmente para a oferta de conexão de dados a seus usuários finais;

Esta Normativa tem por objetivo estabelecer condutas e procedimentos para a promoção da segurança cibernética nas redes e serviços de telecomunicações prestados pela FIBRASIL. A Normativa deve orientar a conduta de seus empregados e dos *stakeholders* que se relacionam com a FIBRASIL, com intuito de alcançar o fim desejado.

2. APLICAÇÃO

Aplica-se aos empregados, aos clientes e aos fornecedores da FIBRASIL, bem como às demais partes interessadas que mantenham relação com a FIBRASIL.

3. ACRÔNICOS E ABREVIATURAS

As siglas e acrônimos aqui utilizados seguem a Portaria Número 93, de 26 de setembro de 2019, do GSI (Glossário de Segurança da Informação).

4. PRINCÍPIOS E DIRETRIZES

A segurança é um dos princípios fundamentais em que se apoia a presente Normativa e ela se divide em segurança integral e segurança digital.

A segurança integral engloba não apenas a segurança física e operacional (de pessoas e bens) mas também a continuidade do negócio, a prevenção da fraude, bem como qualquer outro âmbito ou função relevante cujo objetivo seja a proteção corporativa frente a potenciais prejuízos, sejam quais forem, ou eventuais perdas.

Por sua vez, o conceito de segurança digital integra os aspectos relacionados à segurança da informação[1] e segurança cibernética. Esses aspectos serão aplicáveis aos suportes, sistemas e tecnologias e elementos que compõem a Rede. As disposições de segurança aplicáveis aos ativos

[1] Este tema é tratado em Normativa própria.

da FIBRASIL serão projetadas também sobre suas entidades colaboradoras (fornecedores, terceirizados etc.) quando a atividade destas afete àquele no desenvolvimento do seu negócio.

Além do princípio da segurança, as ações da FIBRASIL para a promoção da Segurança Cibernética nas redes e serviços de telecomunicações devem buscar assegurar os seguintes princípios:

- Princípio de legalidade;
- Autenticidade;
- Confidencialidade;
- Disponibilidade;
- Diversidade;
- Integridade;
- Interoperabilidade;
- Prioridade;
- Responsabilidade; e,
- Transparência.

Os empregados envolvidos direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações da FIBRASIL devem atuar em Segurança Cibernética observando as seguintes diretrizes:

- Adotar normas e padrões e referências de boas práticas em Segurança Cibernética;
- Atuar com responsabilidade, zelo e transparência;
- Disseminar a cultura de Segurança Cibernética;
- Buscar a utilização segura e sustentável das redes e serviços de telecomunicações;
- Identificar, proteger, diagnosticar, responder e recuperar de incidentes de Segurança Cibernética;
- Empenhar esforços para mitigar os riscos cibernéticos;
- Respeitar e promover os direitos humanos e as garantias fundamentais;
- Empenhar esforços para que sejam adotados conceitos de *security by design* e *privacy by design* no desenvolvimento e aquisição de produtos e serviços no setor de telecomunicações.

5. AÇÕES

Com vistas a garantir um ambiente seguro, são desenvolvidas as seguintes ações:

i. Processos formais de educação continuada e planos de capacitação e disseminação sobre o que é segurança cibernética, quais são os riscos envolvidos na operação e como cada área e

colaboração deve agir diante de um incidente. Tais processos e metodologias são desenvolvidas para os colaboradores e *stakeholders* envolvidos direta ou indiretamente em atividades que contribuam para a cultura de segurança cibernética dentro da organização, e serão revisados periodicamente;

ii. Procedimentos relativos ao armazenamento seguro dos dados pessoais, conforme tratado conforme Normativas de Segurança da Informação e de Proteção de Dados Pessoais da FIBRASIL;

iii. Os procedimentos e controles adotados para a identificação e a análise das vulnerabilidades, das ameaças e dos riscos associados à Segurança Cibernética e à continuidade dos serviços de telecomunicações, conforme normativa de Análise de Vulnerabilidades da FIBRASIL;

iv. O mapeamento de possíveis riscos de incidentes e de eventos que possam afetar a segurança do armazenamento de dados, conforme normativas de Segurança da Informação e de Proteção de Dados Pessoais da FIBRASIL. Os procedimentos e controles adotados para mitigar as vulnerabilidades identificadas, conforme normativa de Análise de Vulnerabilidades da FIBRASIL;

v. O plano de resposta a incidentes, conforme normativa de Resposta a Incidentes da FIBRASIL.

vi. Os procedimentos relativos ao compartilhamento de informações sobre incidentes relevantes e outras informações relativas à Segurança Cibernética, conforme normativa de Resposta a Incidentes da FIBRASIL.

6. PAPEIS E RESPOSABILIDADES

6.1. COMITÊ DE SEGURANÇA CIBERNÉTICA

O Comitê de Segurança Cibernética é composto por um representante de cada uma das seguintes áreas:

- Gerência Regulatória e Institucional;
- Gerência de Operações;
- Gerência de Governança;
- Gerência de Infraestrutura e Segurança de TI;
- Gerência de *Site Management;*Gerência de Projetos e Desenvolvimento TI.

Após indicação, os representantes são aprovados por Reunião de Diretoria (REDIR).

Caberá ao Comitê desempenhar as seguintes funções:

- Compartilhar conhecimento, iniciativas e planos relacionados à segurança cibernética;

- Discutir, avaliar, revisar e propor para as áreas responsáveis ações para o cumprimento desta Normativa;
- Propor para as áreas responsáveis padrões e requisitos mínimos de Segurança Cibernética nos ambientes de telecomunicações;
- Analisar e contribuir com planos de ação e controles relacionados a riscos de Segurança Cibernética;
- Atualizar o diretor responsável pela Normativa de Segurança Cibernética sobre as atividades e propostas discutidas no presente Comitê.

6.2. DIRETOR(A) RESPONSÁVEL PELA NORMATIVA DE SEGURANÇA CIBERNÉTICA

O *Chief Technology Information Officer* será o(a) diretor(a) responsável pela Normativa de Segurança Cibernética.

Caberá ao Diretor:

- Supervisionar a implementação dos planos de ação relacionados ao tema de Segurança Cibernética;
- Reportar aos demais Diretores Estatutários da FIBRASIL eventos relacionados a violações desta Política;
- Acompanhar as ações do Comitê de Segurança Cibernética;
- Representar, juntamente com a Gerência Regulatória e Institucional, a FIBRASIL perante as autoridades administrativas quando se tratar de algum tema relacionado à presente Normativa;
- Acompanhar as denúncias de incidentes relacionados à segurança cibernética.
- Cumprir e fazer cumprir as Políticas e Normas de Segurança.

6.3. OPERAÇÕES

O NOC, Network Operation Center ou Centro de Operação de Rede, monitora os principais dispositivos de redes, aplicações e serviços que estão conectados à infraestrutura da FIBRASIL. Possui em sua estrutura, profissionais especializados que monitoram a Rede da FIBRASIL em regime 24x7x365. Suas principais responsabilidades são:

- Monitoração e desempenho de rede, acionamentos técnicos, análise de causa raiz, gestão do SLA das falhas e Suporte à equipe de campo.
- Gestão fim a fim de todos os alarmes e falhas na Rede FIBRASIL, para garantia da prestação do serviço contratado por seus clientes;

- Escalonamento de Incidentes fora do SLA;
- Acompanhamento de Atividades Programadas;
- Atendimento aos clientes da FIBRASIL e ações para restabelecimento das falhas de seus usuários finais;
- Análise de problemas (GPROB), definição de ações de melhoria, implementação e ajustes de processos operacionais;
- Gestão de Vulnerabilidades
- Gestão de Patch
- Adotar, certificar e executar as melhores práticas de segurança.

Além do NOC, a FIBRASIL conta com o Centro de Operações de Segurança (SOC), que combina conhecimentos humanos, processuais e tecnológicos com objetivo de detecção e reação aos eventuais incidentes de segurança.

O SOC é exclusivamente focado na Segurança onde através de eventos, alertas e dashboards é realizada a monitoração para garantir a proteção dos ativos e serviços da empresa. Foco total em garantir a tríade da Segurança: Disponibilidade, Integridade e Confidencialidade.

As principais atribuições do SOC são:

- CSIRT: *Computer Security Incident Response Team* ou Grupo de Resposta a Incidentes de Segurança: especialista que recebe, analisa e responde as notificações e atividades relacionadas a problemas de Cibersegurança.
- *Playbooks/runbooks*: Tem como objetivo evoluir os procedimentos estratégicos definidos para os incidentes de segurança;
- *Hardening:* Tem como objetivo analisar as configurações, recomendar boas práticas e verificar as conformidades dos elementos de rede.
- Gestão de Vulnerabilidade: Tem como objetivo a identificação, classificação e priorização de vulnerabilidades dentro do ambiente.
- Gestão de *Patch*: Tem como objetivo administrar as atualizações dos sistemas operacionais, plataformas e aplicações em uso na empresa.
- Monitoração contínua: Tem como objetivo analisar e gerenciar eventos de Segurança alarmados na plataforma SIEM.

- Indicadores de comprometimento: Tem como objetivo acompanhar a existência de violações de segurança dispositivos e sistemas que comprometam a segurança da nossa rede ou sistemas.

6.4. SISTEMAS TI

A área de Sistema de TI tem a missão de monitorar os sistemas de OSS/BSS para prover o devido funcionamento de todos os serviços para os clientes da FIBRASIL. A equipe conta com especialistas com atuação nos seguintes pilares estratégicos:

- Sustentação – Garantir o funcionamento de todas as aplicações/serviços 24X7. Neste pilar, a área tem a missão de monitorar todas as aplicações, ordens e atuar de forma preventiva antes de qualquer acionamento das Operações:
  i. Monitoramento das aplicações;
  ii. Gestão de sala de Crises;
  iii. Gestão dos chamados/incidentes/SLAs;
- Arquitetura – Garantir o desenho e evolução dos sistemas de forma escalável e sustentável em prol de soluções altamente tecnológicas e digitais. A arquitetura dos sistemas da FIBRASIL é embasada pelo padrão recomendado pelo mercado de TMForum, garantindo alta performance nas camadas integradoras:
  i. Análises de integrações/soluções;
  ii. Desenho de soluções;
  iii. Documentação do eco sistema de forma integrada com todas as camadas;
- Projetos – Garantir a implementações de novas iniciativas, melhorias e correções de causa raiz em nossos sistemas. Neste pilar, a função é construir soluções com olhar 360 junto as áreas de negócio para garantir soluções aderente que alavanque os resultados em receitas e otimize em prol de eficiências operacionais:
  i. Acompanhamento dos projetos;
  ii. Atendimento das áreas de negócio e dos clientes da FIBRASIL;
  iii. Gestão das entregas;
  iv. Acompanhamento dos indicadores dos projetos;
  v. Validações das soluções;
  vi. Gestão das CR’s.

7. MEDIDAS CORRETIVAS

O empregado da FIBRASIL ou terceiro que identificar algum incidente que afete à Normativa[2], potencial ou efetivo, ainda que sob suspeita, deverá comunicar imediatamente, por meio do e-mail incidentes@fibrasil.com.br, ou via ticket no portal de *helpdesk* https://helpdesk.fibrasil.com.br

Todas as comunicações de incidentes serão mantidas em confidencialidade, tanto pelo empregado que as reportou como pelos responsáveis pela condução das medidas de enfrentamento, de forma a preservar a identidade do empregado e a conter os riscos decorrentes do incidente, exceto quando a sua divulgação for expressamente exigida por lei ou autoridade governamental.

Uma vez identificado um incidente, potencial ou efetivo, ainda que sob suspeita, caberá a área responsável pelo tratamento do incidente (o incidente pode ser de operações de rede ou de TI) da FIBRASIL tomar as seguintes medidas:

i. Avaliar e registrar internamente o incidente, identificando-o e classificando-o quanto a (i) probabilidade de ocorrência, (ii) impacto e (iii) nível de gravidade.
ii. Adotar e fazer com que sejam adotadas as respostas imediatas cabíveis, quando assim necessárias para a contenção do incidente e mitigação dos riscos envolvidos.
iii. Indicar (i) as medidas corretivas e/ou mitigatórias a serem adotadas, (ii) o responsável interno por implementá-las, e (iii) o prazo para a implementação.
iv. Comunicar o incidente à Gerência Regulatória e Institucional quando houver necessidade de comunicar autoridades governamentais por força da lei;
v. Investigar as causas raízes do incidente, adotando medidas forenses de preservação de evidências, levantamento e recuperação de dados e registro em cadeia de custódia.
vi. Emitir relatório contendo a conclusão das investigações e as medidas de enfrentamento adotadas.
vii. Rever e propor medidas de melhorias nos processos e controles na gestão de segurança da informação com base no incidente experimentado.

Todos os incidentes, sem exceção e independentemente de serem potenciais ou efetivos, deverão ser registrados na matriz de risco da FIBRASIL, que será elaborada pelas áreas de Governança CTIO e Controles Internos da FIBRASIL, para fins do monitoramento das vulnerabilidades e correto enfrentamento.

[2] Os incidentes de segurança da informação, os incidentes envolvendo dados pessoais, bem como as vulnerabilidades identificadas, são tratadas em Normativas específicas, conforme listadas no item 5 da presente Normativa.

8. DOCUMENTOS RELACIONADOS

Além desta Normativa, aplicam-se as seguintes legislações e normas:

- Todas as Políticas Corporativas da FIBRASIL;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD;
- Lei nº 12.965/2014 (Marco Civil da Internet) e o Decreto nº 8.771/2016;
- Resolução nº 740/2020 da Anatel (Regulamento de Segurança Cibernética) e demais normas que dispõem sobre o tema;
- Normativa de Segurança da Informação;
- Normativa de Privacidade e Proteção de Dados Pessoais;
- Normativa de Análise de Vulnerabilidade.
- Normativa de Resposta a Incidentes

Sem prejuízo das demais leis e regulamentos setoriais que disponham sobre o tema.

9. VIGÊNCIA

A presente normativa terá validade a partir da data de sua aprovação e permanecerá em vigor até sua expressa revogação.